ENDPOINT PROTECTOR

User Manual Version 1.0.0.9

Mobile Device Management (MDM) User Manual

COSOSYS

Table of Contents

1. Introduction 1
1.1. What is Endpoint Protector? 2
2. Activation of Mobile Device Management 3
2.1. Activation of Mobile Device Management Feature 4
3. How Endpoint Protector MDM Works 5
3.1. Supported Operating Systems and devices 6
4. MDM Setup APNS (Apple) & GCM (Google Android) 7
4.1. Setup of APNS for iOS and OS X 8
4.1.1. What is an Apple APNS Certificate and why do I need it? 8
4.1.2. How to generate your Apple APNS Certificate? 9
4.1.3. Renew an Apple APNS Certificate before expiration 11
4.2. Setup of GCM for Android 16
4.2.1. What is GCM (Google Cloud Messaging) and why I need it? 16
4.2.2. How to get your Google API Key for GCM and Maps?-new method (April 2014) 17
4.2.3. Entering Google API Key and Project Number in Endpoint Protector-new method 21
4.2.4. How to get your Google API Key for GCM and Maps?-old method 22
4.2.5. Entering Google API Key and Project Number in Endpoint Protector-old method 25
4.2.6. Google C2DM 26
5. iOS EPP MDM App 27
5.1. EPP MDM iOS App Supported iOS Versions 27
5.2. EPP MDM iOS App to locate devices 27
5.3. EPP MDM iOS App to enroll devices (optional) 28
5.4. EPP MDM iOS App Device Information 28
5.5. Installing the EPP MDM iOS App 29
5.6. Allow Location Services for EPP MDM iOS App 30
5.7. Pushing and Managing EPP MDM App to iOS Devices 30

6. Android Endpoint Protector MDM Client App 31
6.1. EPP MDM Android Client App Supported Versions 31
6.2. The Android EPP Client App 31
6.3. EPP Client Android App to enroll devices 31
6.4. Install EPP Client App on Android and Enrolling Android Device 32
7. Enrolling Mobile Devices 38
7.1. Different Enrollment methods are available: 39
7.2. Mobile Device Enrollment 40
7.2.1. iOS and OS X Enrollment and Profile Protection 43
7.2.2. iOS and OS X Profile Protection Deletion Passphrase 44
7.2.3. Sending E-Mail or SMS Enrollment Invitation (iOS/OS X / Android) 46
7.2.4. SMS Enrollment Number Format (iOS / Android) 46
7.2.5. E-Mail Enrollment Invitation (iOS/OS X / Android) 47
7.2.6. SMS Enrollment Invitation (iOS / Android) 48
7.2.7. iOS and OS X Mobile Device Enrollment over URL 49
7.2.8. iOS Mobile Device Enrollment through EPP MDM App 51
7.2.9. Android Device Enrollment 54
7.2.10. Bulk Enrollment 54
8. Managing Mobile Devices 58
8.1. Mobile Device Status 60
8.1.1. Available Options 63
9. Manage iOS Devices 65
9.1. Security Settings (Security Profile) on iOS 65
9.1.1. Password / Passcode Setting on iOS Device 66
9.1.2. Clear Passcode (No more password required) 66
9.1.3. iOS Device Hardware Encryption 66
9.2. Restrictions (Restrictions Profile) on iOS 67
9.2.1. The following iOS features can be restricted 68
9.2.2. The following Applications can be restricted 69
9.2.3. iCloud restrictions / Photo stream restrictions 69
9.2.4. Security and Privacy Restrictions 69
9.2.5. Content Rating Restrictions 69
9.2.6. iOS7 Restrictions 70

9.2.7. Supervised Device Restrictions 70
9.3. Remote iOS Lock of Device 70
9.4. Remote iOS Device Wipe (Device Nuke) 71
9.5. iOS Disable Device Password / Passcode 72
9.6. Device Ownership 72
9.7. Voice Roaming on iOS 72
9.8. Data Roaming on iOS 73
9.9. Profile Removal Policy for iOS Devices 73
9.10. Refresh Device Details for iOS 74
9.11. Refresh App List for iOS 74
9.12. Installed Apps on iOS 75
9.13. Refresh Profile List on iOS 75
9.14. Profiles on iOS Devices Information 75
9.14.1. Remove Profile from iOS Device 76
9.15. Manage WiFi on iOS 76
9.15.1. Wipe Wi-fi Settings 77
9.16. Manage Mail on iOS 77
9.16.1. Wipe E-mail Settings 77
9.17. Exchange Active Sync 77
9.18. Manage VPN on iOS 78
9.19. Manage APN settings on iOS 78
9.20. Manage Cellular Settings on Supervised iOS 7 devices 79
9.21. App Lock on Supervised iOS 7 devices 79
9.22. Installed Apps 80
9.23. History of iOS Devices Actions 80
9.24. History Location 81
10. Manage OSX Devices 82
10.1. Security Settings (Security Profile) on OS X 82
10.1.1. Password / Passcode Setting on OS X Device 83
10.1.2. OS X Device Hardware Encryption 83
10.2. File Vault 2 Disk Encryption on OS X 83

10.2.1. Disk Encryption Status 85
10.3. Remote Lock of Device 85
10.4. Remote OS X Device Wipe (Device Nuke) 85
10.5. Device Ownership 86
10.6. Profile Removal Policy for OS X Devices 86
10.7. Refresh Device Details for OS X 87
10.8. Refresh App List for OS X 87
10.9. Installed Apps on OS X 87
10.10. Refresh Profile List on OS X 88
10.11. Profiles on OS X Devices Information 88
10.11.1. Remove Profile from OS X Device 88
10.12. Manage WiFi on OS X 89
10.12.1. Wipe Wi-fi Settings 89
10.13. Manage Mail on OS X 89
10.13.1. Wipe E-mail Settings 90
10.14. Manage VPN on OS X 90
10.15. History of OS X Devices Actions 91
11. Manage Android Devices 92
11.1. Security Settings (Security Profile) on Android 92
11.1.1. Password / Passcode Setting on Android Device 93
11.1.2. Device Password 94
11.1.3. Android Device Hardware Encryption 94
11.2. Request Storage Encryption 95
11.3. Remote Android Lock of Device 95
11.4. Remote Android Device Wipe (Device Nuke) 96
11.4.1. Android Remote Wipe of SD-Card 96
11.5. Device Ownership 97
11.6. Android Device Location Settings 97
11.6.1. Location Accuracy Fine on Android 98
11.6.2. Location Cost Allowed on Android 98
11.7. Manage Wifi 98
11.8. Manage Bluetooth 98

11.9. Manage Camera on Android 99
11.10. Play Sound on Device for Android 99
11.11. Refresh Google Accounts for Android 100
11.12. Refresh Device Details for Android 100
11.13. Refresh App List for Android 100
11.14. Manage Calendar Events 101
11.15. Installed Apps on Android 102
11.15.1. Removing Installed Apps on Android 102
11.16. Get Contacts on Android 103
11.17. Get Accounts on Android 103
11.18. History of Android Device Actions 103
11.19. Manage WiFi, Manage Mail, Profiles on Android 104
12. Mobile Application Management (MAM) for iOS 105
12.1. Adding Apps to your Managed Apps Catalog 106
12.1.1. Searching for Apps 106
12.1.2. Adding Apps to Managed Apps Catalog 107
12.1.3. Adding „Enterprise Apps" to Managed Apps Catalog 107
12.2. Editing App Management Options 108
12.3. Managed Paid Apps 110
12.4. Pushing Apps to iOS Devices 112
12.4.1. Update Managed Apps / Changing Settings 113
12.5. Removing Managed Apps from iOS Devices 114
13. Android App Management 115
13.1. Adding Apps to your Managed Apps Catalog 116
13.2. Editing App Management Options 116
13.3. Pushing Apps to Android Devices 117
13.4. Removing Managed Apps from Android Devices 118
14. Policy Builder for iOS, OSX or Android Devices 119
14.1. Create a Policy for iOS, OS X or Android Devices 120

14.2. Assigning Devices to Policy 121
15. Unmanage a Mobile Device / Uninstall App 122
15.1. iOS and OS X Device Unmanage by Administrator (over-the-air) 122
15.1.1. iOS Uninstall / Unmanage by User (on Device) 122
15.1.2. OS X Uninstall / Unmanage by User (on Device) 123
15.2. Uninstall iOS EPP MDM app 123
15.3. Android EPP Client App Uninstall / Unmanage Android Device123
16. GeoFencing 128
16.1. How to setup a GeoFence..... 129
16.2. How to deploy MDM Policies using Geofences 130
17. Installing Root Certificate to your Internet Browser 131
17.1. For Microsoft Internet Explorer 131
17.2. For Mozilla Firefox..... 139
18. Terms and Definitions 141
18.1. Server Related..... 141
18.2. Client Related..... 142
19. Support 143
20. Important Notice / Disclaimer..... 144

1. Introduction

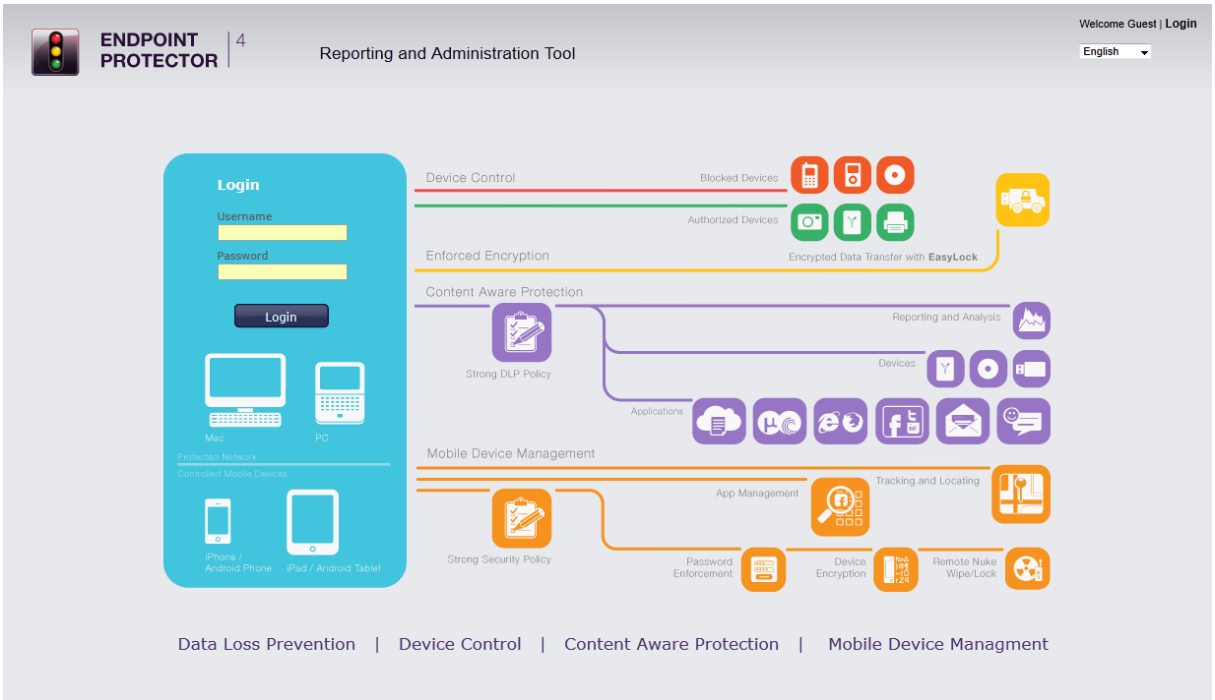
In the last past years, mobile devices have invaded business environments. Personally owned or company owned smartphones and tablets are used on a daily basis by employees to store and have access to their company e-mails, sales reports etc. everywhere they go.

The wide adoption of the BYOD (Bring-Your-Own-Device) model by companies worldwide led to the use of more personal mobile devices by employees for storing business information together with private data such as photos and music. This trend raised new issues for IT administrators, which are faced now with the challenge of protecting sensitive company data not only inside the secured company network, but also everywhere it is taken on mobile company endpoints. At the same time, a separation and close monitoring of company information from personal data must be imposed.

To face the security challenges by the increase mobility in business environments, Mobile Device Management by Endpoint Protector enables a complete control and detailed monitoring over the use of mobile devices both inside and outside corporate environments, allowing employees to have a secure access to both corporate and private data wherever they are and on whatever device they are using without business critical information getting compromised.

1.1. What is Endpoint Protector?

Endpoint Protector is a complete Data Loss Prevention solution for companies' networks of all sizes, enabling a detailed control over removable, mobile storage media and mobile devices both inside and outside the companies' walls.



Endpoint Protector comprises three separate modules, which used together ensures the next generation security of your endpoints:

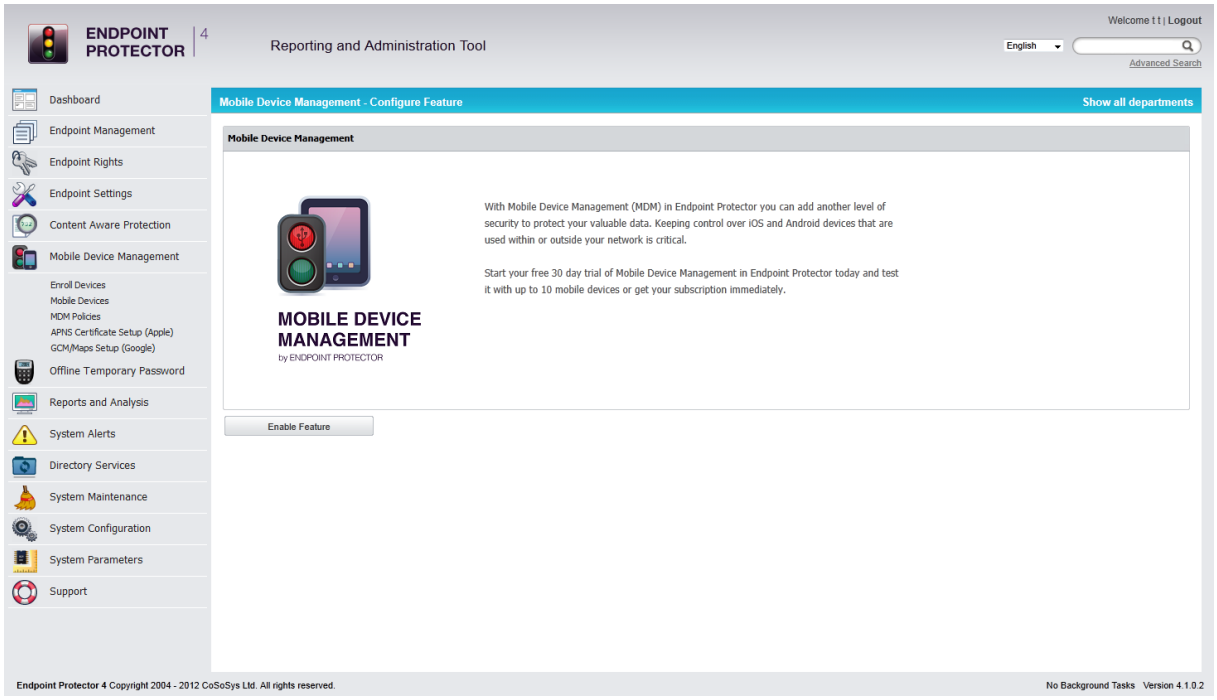
- **Mobile Device Management**: closely controls and monitors the entire mobile device fleet through dedicated MDM policies, protecting sensitive company data, while permitting a degree of freedom on what concerns the stored personal information. Once integrated in a company or enterprise network, it ensures a highly secure working environment for companies adopting and using the BYOD model.

- **Device Control**: enforces strong security policies for controlling and closely monitoring all portable storage device use inside the company network. Once deployed inside companies networks, the Device Control modules reduces the risks of data loss and data theft through unauthorized use of removable and mobile devices through USB, etc..

- **Content Aware Protection**: allows defining custom content aware policies for a detailed inspection, detection and reporting of all sensitive content transfers outside the secured network. Once enabled, the Content Aware Protection module scans all possible exit points and ensures that no critical data leaves the company network either by transfers to removable media or directly via e-mail, file sharing applications or to the cloud.

2. Activation of Mobile Device Management

The Mobile Device Management feature enables administrators to remotely control and enforce strong security policies on iOS/OS X (Apple) and Android devices. Through options such as remote data wipe, device tracking and blocking, it offers enhanced protection against data theft and data loss, considerably reducing the risks that come with the increase of mobility in today's business environment.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome t t | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection
Mobile Device Management
Enroll Devices
Mobile Devices
MDM Policies
APNS Certificate Setup (Apple)
GCM/Maps Setup (Google)
Offline Temporary Password
Reports and Analysis
System Alerts
Directory Services
System Maintenance
System Configuration
System Parameters
Support
Mobile Device Management - Configure Feature
Show all departments
Mobile Device Management
MOBILE DEVICE MANAGEMENT
by ENDPOINT PROTECTOR
With Mobile Device Management (MDM) in Endpoint Protector you can add another level of security to protect your valuable data. Keeping control over iOS and Android devices that are used within or outside your network is critical.
Start your free 30 day trial of Mobile Device Management in Endpoint Protector today and test it with up to 10 mobile devices or get your subscription immediately.
Enable Feature
Endpoint Protector 4 Copyright 2004 - 2012 CoSoSys Ltd. All rights reserved.
No Background Tasks Version 4.1.0.2

2.1. Activation of Mobile Device Management Feature

Mobile Device Management comes as an optional feature with Endpoint Protector that requires a yearly-based separate subscription based on the number of protected mobile devices. By default, the feature appears as deactivated inside the Endpoint Protector Reporting and Administration interface.

The Mobile Device Management feature requires an internet connection for the Endpoint Protector Appliance.

The feature can be enabled by simply selecting the Mobile Device Management option from the left-side menu and clicking on the Enable Feature button.

Activating this feature will require a working Internet connection on Endpoint Protector Server/Appliance. Additionally, the initiator of the activation request will have to provide several company details such as Company Name, Contact Person Name and Contact Details, which will be sent to the Endpoint Protector Licensing Server including: Company name, Contact Person, Contact Details (phone number and e-mail). CoSoSys will use this information only for validation purposes and it will not imply subscribing to any newsletter or sharing it with any third party.

Once the request was processed and approved, the feature will be enabled by the CoSoSys Team. A notification will be sent to the provided e-mail address and the trial period for the feature will be activated.

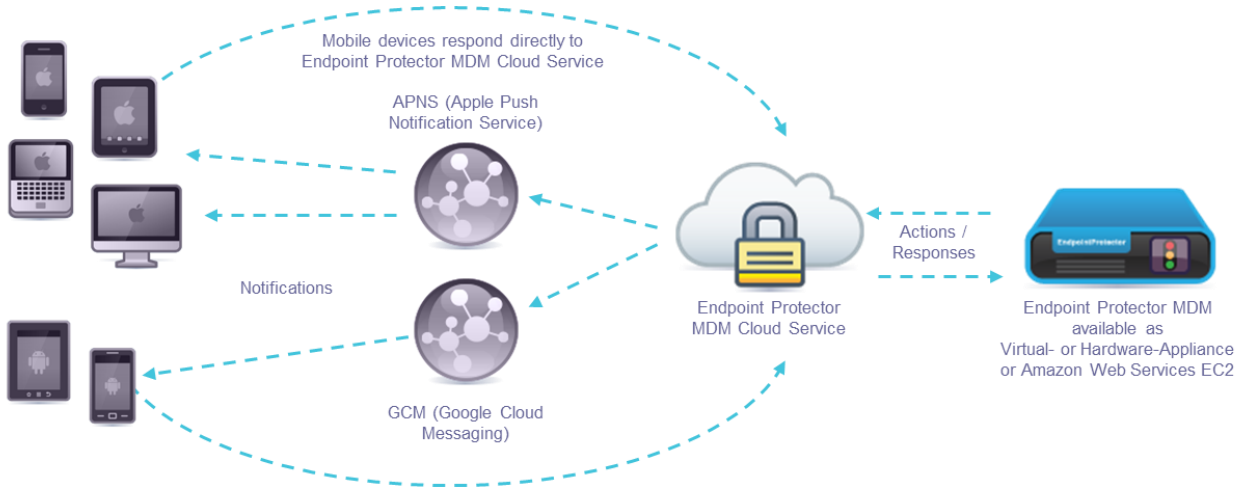
Please make sure your Firewall will have domains @cososys.com and @endpointprotector.com whitelisted for you to receive all communication.

A yearly subscription can be purchased to further use all the functionalities of the Mobile Device Management feature.

3. How Endpoint Protector MDM Works

For Endpoint Protector Mobile Device Management to be able to manage your mobile iOS, OS X and Android devices the communication between the devices and the Endpoint Protector Appliance over an internet connection is vital. Management actions need to arrive at your device either by a data connection like 3G in case of an iPhone or over an internet connection if the device does not have a data connection like an iPad (with Wi-Fi only), an Android tablet or a MacBook.

For the management actions to arrive at the device the actions are sent using for iOS and OS X devices the Apple Push Notification Service (short APNS) and for Android devices the Google Cloud Messaging Service (short GCM). To simplify the setup of your Endpoint Protector MDM service the Endpoint Protector Cloud is communicating between your Endpoint Protector Appliance (the Administration and Management Server) and the Apple and Google Services with your devices.


Mobile devices respond directly to Endpoint Protector MDM Cloud Service
APNS (Apple Push Notification Service)
Notifications
GCM (Google Cloud Messaging)
Endpoint Protector MDM Cloud Service
Actions / Responses
Endpoint Protector MDM available as Virtual- or Hardware-Appliance or Amazon Web Services EC2

For the communication to work between your mobile devices and Endpoint Protector it is required that you setup the APNS and GCM settings as described in the following steps.

3.1. Supported Operating Systems and devices

The supported mobile device operating systems are:

- iOS7 (iPhone and iPad), iOS6 (iPhone and iPad), iOS5, iOS4
- OS X 10.9.1+
- Android 2.2+ (Codename Froyo) or newer versions
  A list of supported Android mobile devices is not provided due to the large number of devices from different manufacturers. In general Android devices with Android Operating version 2.2 and newer are supported.

4. MDM Setup APNS (Apple) & GCM (Google Android)

Before you can use the Endpoint Protector MDM features for iOS, OS X and Android different settings are required for you to make. The following steps describe the steps and settings needed to be able to communicate between your mobile devices and Endpoint Protector.

Attention!

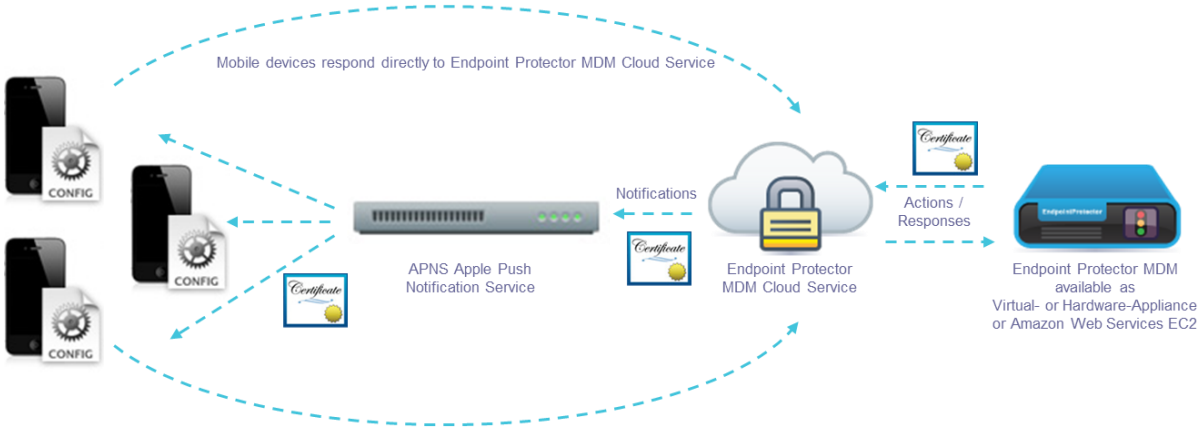
For Endpoint Protector Administrators that want to use the MDM Functionality only with Android devices the Apple APNS Setup (required for MDM with iOS or OS X) is **NOT REQUIRED**. If you want to use Endpoint Protector MDM with iOS/ OS X and Android devices the setup of both GCM (Google Cloud Messaging for Android) and Apple APNS is required.

4.1. Setup of APNS for iOS and OS X

4.1.1. What is an Apple APNS Certificate and why do I need it?

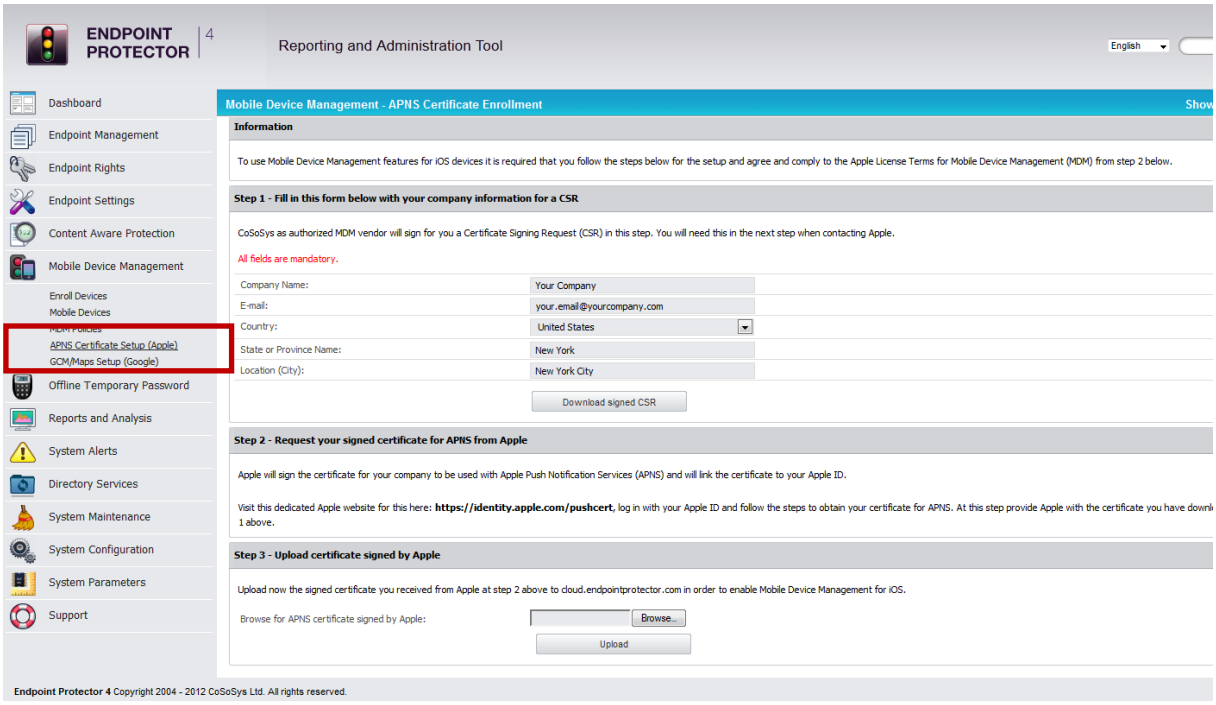
In order to use the MDM features provided for iOS or OS X an Apple Push Notification Service (short APNS) certificate is required by Apple Inc. Receipt of the Apple issued and signed certificate is up to Apple Inc. own discretion.

What is Apple APNS? It is a certificate that is signed by Apple to clearly identify what iOS or OS X devices are communicating with your Endpoint Protector Appliance in order to be sure that only your company own devices receive commands from Endpoint Protector MDM.



4.1.2. How to generate your Apple APNS Certificate?

The APNS Certificate can be generated in just a few simple steps from the Mobile Device Management – APNS Certificate Setup (Apple).


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
English
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection
Mobile Device Management
Enroll Devices
Mobile Devices
APNS Certificate Setup (Apple)
GCM/Maps Setup (Google)
Offline Temporary Password
Reports and Analysis
System Alerts
Directory Services
System Maintenance
System Configuration
System Parameters
Support
Mobile Device Management - APNS Certificate Enrollment
Information
To use Mobile Device Management features for iOS devices it is required that you follow the steps below for the setup and agree and comply to the Apple License Terms for Mobile Device Management (MDM) from step 2 below.
Step 1 - Fill in this form below with your company information for a CSR
CoSoSys as authorized MDM vendor will sign for you a Certificate Signing Request (CSR) in this step. You will need this in the next step when contacting Apple.
All fields are mandatory.
Company Name:
Your Company
E-mail:
your.email@yourcompany.com
Country:
United States
State or Province Name:
New York
Location (City):
New York City
Download signed CSR
Step 2 - Request your signed certificate for APNS from Apple
Apple will sign the certificate for your company to be used with Apple Push Notification Services (APNS) and will link the certificate to your Apple ID.
Visit this dedicated Apple website for this here: https://identity.apple.com/pushcert, log in with your Apple ID and follow the steps to obtain your certificate for APNS. At this step provide Apple with the certificate you have downl
1 above.
Step 3 - Upload certificate signed by Apple
Upload now the signed certificate you received from Apple at step 2 above to cloud.endpointprotector.com in order to enable Mobile Device Management for iOS.
Browse for APNS certificate signed by Apple:
Browse...
Upload
Endpoint Protector 4 Copyright 2004 - 2012 CoSoSys Ltd. All rights reserved.

Note!

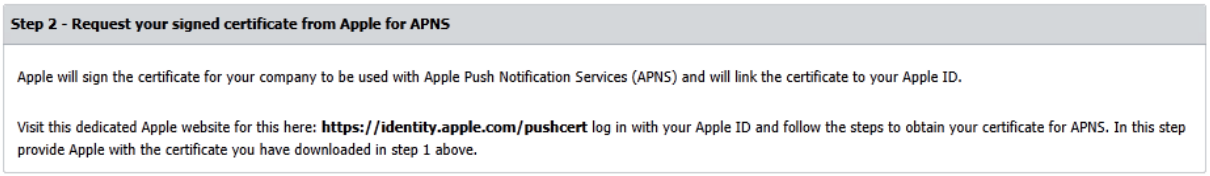
We recommend performing these steps on a Safari or Mozilla Firefox browser. Use of Internet Explorer for this step is known to cause the process to fail.

1. In the Administration Interface, go to Mobile Device Management and select APNS Certificate Setup (Apple), where you have to complete the enrollment for the Apple Push Notification Certificate.

2. Fill in the required details and click on the "Download signed CSR" to get the Code Signing Request (CSR) file signed by CoSoSys. Save it on your computer.

Step 1 - Fill in this form below with your company information for a CSR
CoSoSys as authorized MDM vendor will sign for you a Certificate Signing Request (CSR) in this step. You will need this in the next step when contacting Apple.
All fields are mandatory.
Company Name:
Your Company
E-mail:
your.email@yourcompany.com
Country:
United States
State or Province Name:
New York
Location (City):
New York City
Download signed CSR

3. In a different browser window (Firefox or Safari browser, not Internet Explorer!) open the following link to the Apple Push Certificates Portal: https://identity.apple.com/pushcert/


Step 2 - Request your signed certificate from Apple for APNS
Apple will sign the certificate for your company to be used with Apple Push Notification Services (APNS) and will link the certificate to your Apple ID.
Visit this dedicated Apple website for this here: https://identity.apple.com/pushcert log in with your Apple ID and follow the steps to obtain your certificate for APNS. In this step provide Apple with the certificate you have downloaded in step 1 above.

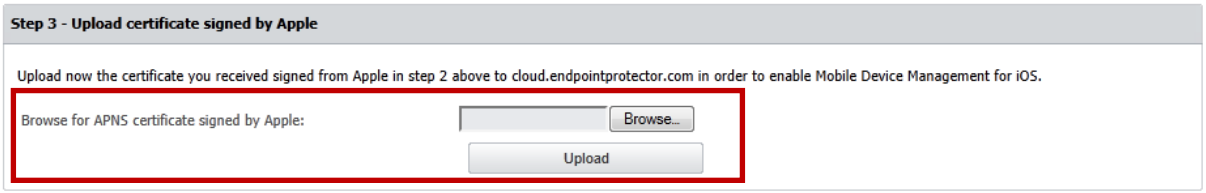
4. Login to the Apple Push Certificates Portal using your Apple ID and follow the steps provided there.

5. Click "Create a Certificate" and agree to the Apple Terms of Use.

6. Select your signed CSR (downloaded at step 2) and click "Upload to the Apple Push Certificates Portal" that you saved on your computer. In just a few moments, your certificate will be available for download.

7. Download now the Certificate from the Apple Push Certificates Portal to your computer.

8. The APNS certificate from the previous step has to be uploaded to the Endpoint Protector MDM Setup.


Step 3 - Upload certificate signed by Apple
Upload now the certificate you received signed from Apple in step 2 above to cloud.endpointprotector.com in order to enable Mobile Device Management for iOS.
Browse for APNS certificate signed by Apple:
Browse...
Upload

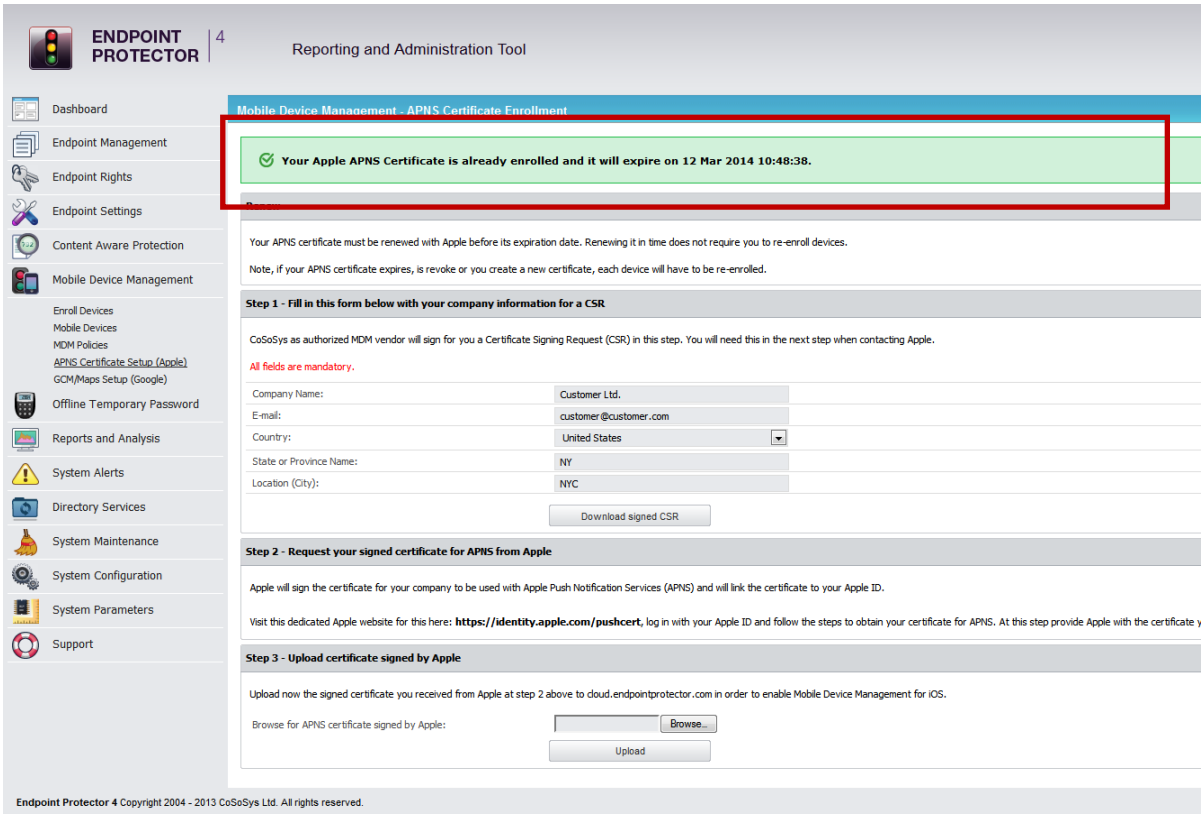
After the upload was successfully performed, your setup for the Endpoint Protector Mobile Device Management is finalized for iOS and OS X.

You can now start enrolling iOS and OS X devices by sending invitations to them either by E-Mail or SMS or through the other supported enrollment methods as described in the following paragraph 7. Enrolling Mobile Devices.

4.1.3. Renew an Apple APNS Certificate before expiration

The Apple APNS certificate must be renewed periodically with Apple before its expiration date to avoid losing control over the managed iOS and OS X devices or having to re-enroll all devices.

Please check the expiration date of your APNS certificate in the Endpoint Protector interface.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection
Mobile Device Management
Enroll Devices
Mobile Devices
MDM Policies
APNS Certificate Setup (Apple)
GCM/Maps Setup (Google)
Offline Temporary Password
Reports and Analysis
System Alerts
Directory Services
System Maintenance
System Configuration
System Parameters
Support
Mobile Device Management - APNS Certificate Enrollment
Your Apple APNS Certificate is already enrolled and it will expire on 12 Mar 2014 10:48:38.
Renew
Your APNS certificate must be renewed with Apple before its expiration date. Renewing it in time does not require you to re-enroll devices.
Note, if your APNS certificate expires, is revoke or you create a new certificate, each device will have to be re-enrolled.
Step 1 - Fill in this form below with your company information for a CSR
CoSoSys as authorized MDM vendor will sign for you a Certificate Signing Request (CSR) in this step. You will need this in the next step when contacting Apple.
All fields are mandatory.
Company Name: Customer Ltd.
E-mail: customer@customer.com
Country: United States
State or Province Name: NY
Location (City): NYC
Download signed CSR
Step 2 - Request your signed certificate for APNS from Apple
Apple will sign the certificate for your company to be used with Apple Push Notification Services (APNS) and will link the certificate to your Apple ID.
Visit this dedicated Apple website for this here: https://identity.apple.com/pushcert, log in with your Apple ID and follow the steps to obtain your certificate for APNS. At this step provide Apple with the certificate
Step 3 - Upload certificate signed by Apple
Upload now the signed certificate you received from Apple at step 2 above to cloud.endpointprotector.com in order to enable Mobile Device Management for iOS.
Browse for APNS certificate signed by Apple:
Browse...
Upload
Endpoint Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved.

The APNS certificate can be renewed in just a few simple steps from the Mobile Device Management – APNS Certificate Setup (Apple) in Endpoint Protector.

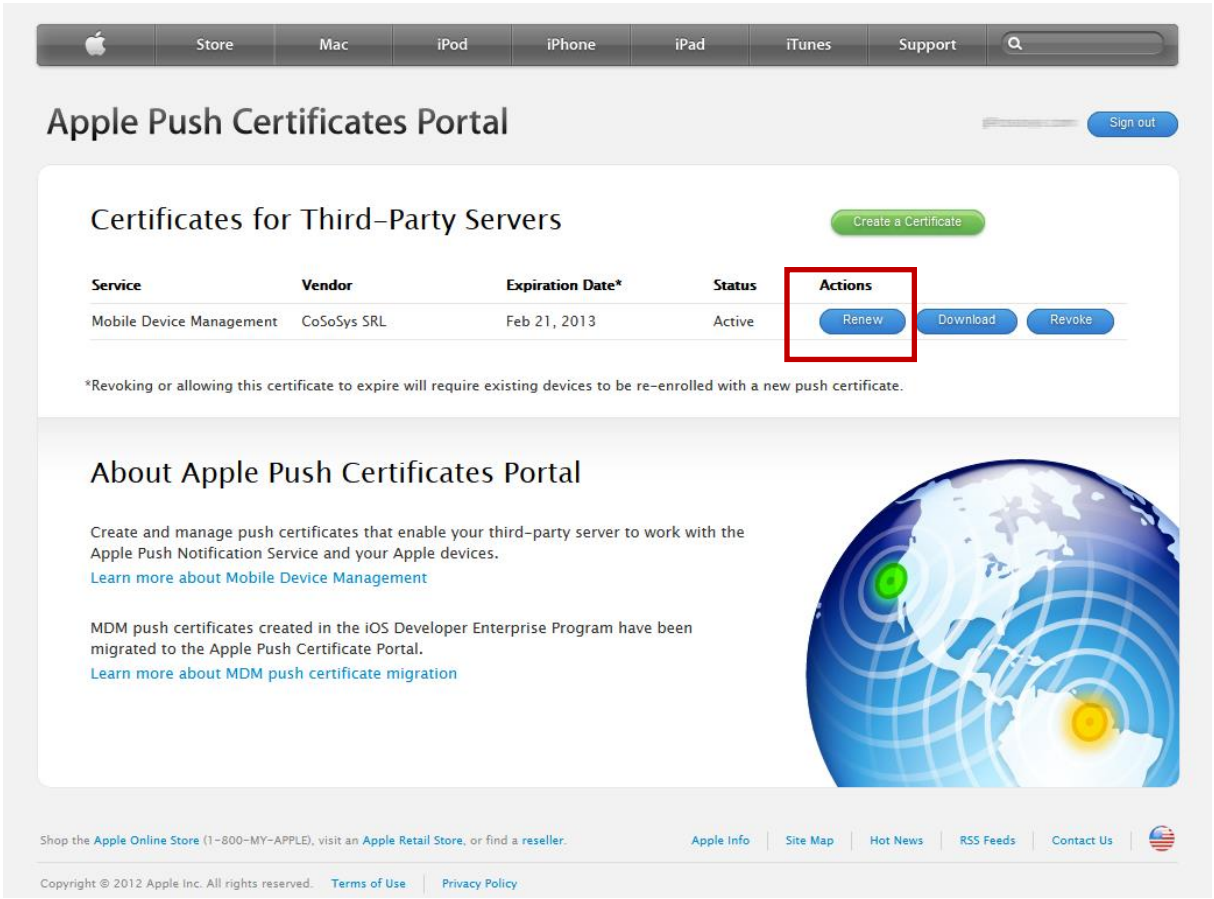
Note!

If your APNS certificate expires or is revoked, it will result in unmanaged iOS and OS X devices. To manage a device after an APNS certificate expires requires re-enroll of the iOS or OS X device.

Note!

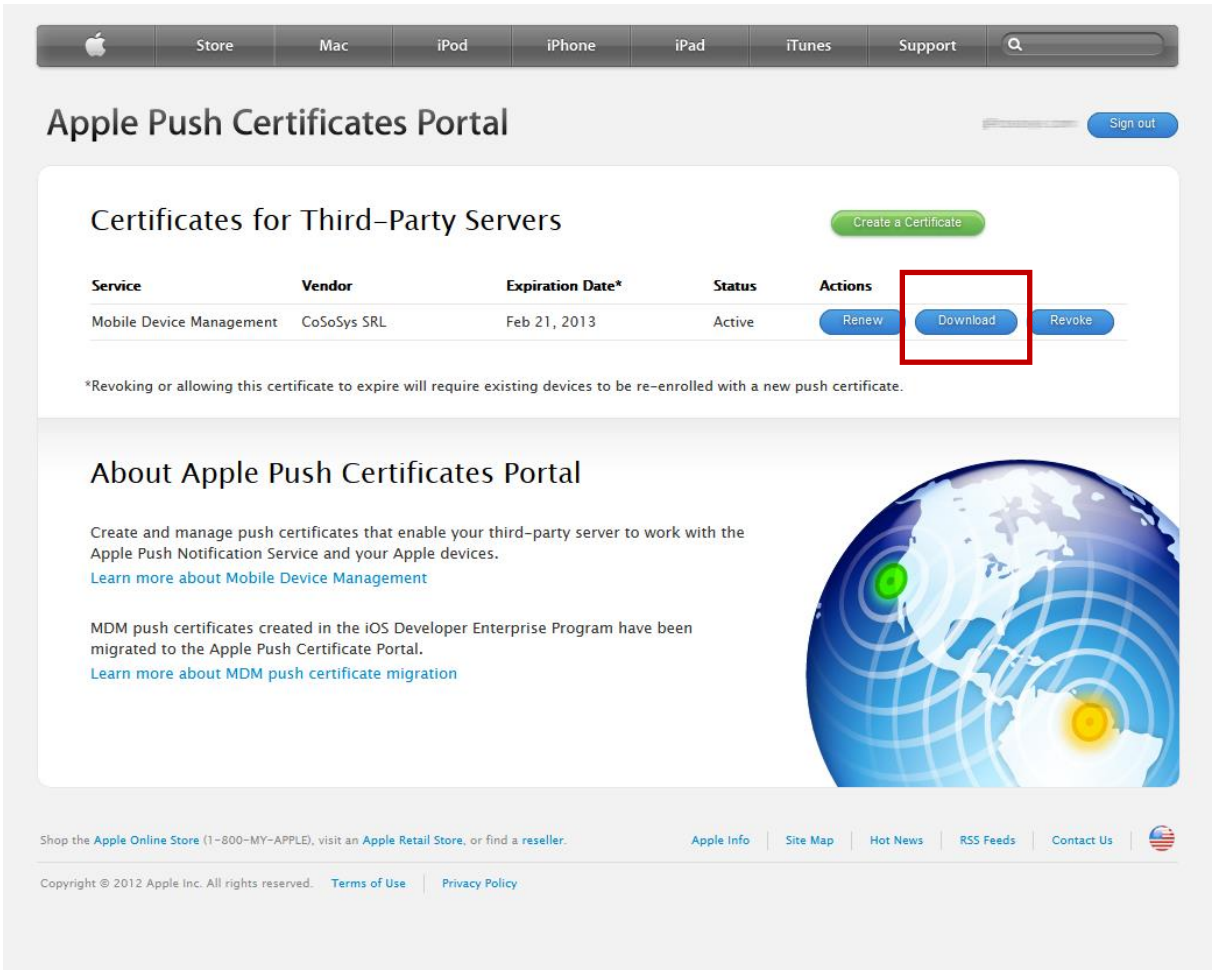
We recommend performing these steps on a Safari or Mozilla Firefox browser. Use of Internet Explorer for this step is known to cause the process to fail.

1. In the Endpoint Protector Administration Interface, go to Mobile Device Management and select APNS Certificate Setup (Apple) setup.
2. Renew your APNS Certificate before it expires by checking the expiration date as mentioned in the interface.
3. Follow the same steps as you have in the initial enrollment process. Click on the "Download signed CSR" to get the Code Signing Request (CSR) file signed by CoSoSys. Save it on your computer.
4. In a different browser window (Firefox or Safari browser, not Internet Explorer!) open the following link to the Apple Push Certificates Portal: https://identity.apple.com/pushcert/
5. Login to the Apple Push Certificates Portal using your Apple ID (previously used to request an APNS Certificate) and follow the steps provided there.
6. Click "Renew".

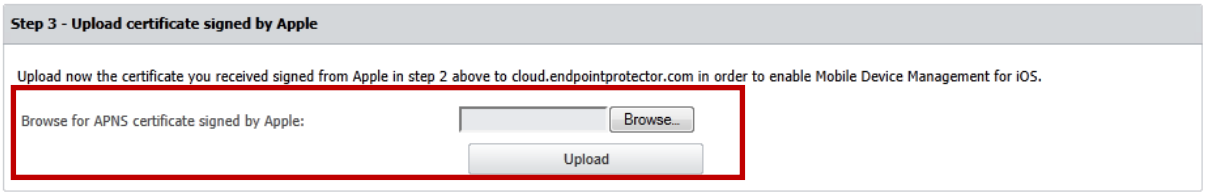

Store
Mac
iPod
iPhone
iPad
iTunes
Support
Apple Push Certificates Portal
Sign out
Certificates for Third-Party Servers
Create a Certificate
Service
Vendor
Expiration Date*
Status
Actions
Mobile Device Management
CoSoSys SRL
Feb 21, 2013
Active
Renew
Download
Revoke
*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.
About Apple Push Certificates Portal
Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices.
Learn more about Mobile Device Management
MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.
Learn more about MDM push certificate migration
Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.
Apple Info
Site Map
Hot News
RSS Feeds
Contact Us
Copyright © 2012 Apple Inc. All rights reserved.
Terms of Use
Privacy Policy

7. After clicking "Renew" you are prompted to upload the Code Signing Request (CSR) from the previous step 3 that you saved on your computer. Select your signed CSR and click "Upload to the Apple Push Certificates Portal". In just a few moments, your certificate will be renewed and you see the Expiration date is updated.

8. Download now the Certificate from the Apple Push Certificates Portal to your computer.


Store
Mac
iPod
iPhone
iPad
iTunes
Support
Apple Push Certificates Portal
Sign out
Certificates for Third-Party Servers
Create a Certificate
Service
Vendor
Expiration Date*
Status
Actions
Mobile Device Management
CoSoSys SRL
Feb 21, 2013
Active
Renew
Download
Revoke
*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.
About Apple Push Certificates Portal
Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices.
Learn more about Mobile Device Management
MDM push certificates created in the iOS Developer Enterprise Program have been migrated to the Apple Push Certificate Portal.
Learn more about MDM push certificate migration
Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.
Apple Info
Site Map
Hot News
RSS Feeds
Contact Us
Copyright © 2012 Apple Inc. All rights reserved.
Terms of Use
Privacy Policy

9. The APNS certificate from the previous step has to be uploaded to the Endpoint Protector/My Endpoint Protector MDM Setup.


Step 3 - Upload certificate signed by Apple
Upload now the certificate you received signed from Apple in step 2 above to cloud.endpointprotector.com in order to enable Mobile Device Management for iOS.
Browse for APNS certificate signed by Apple:
Browse...
Upload

After the upload was successfully performed, your APNS renewal for the Mobile Device Management is finalized.

Please check if the expiration date of the APNS certificate in Endpoint Protector/My Endpoint Protector was updated to the renewed date.

4.2. Setup of GCM for Android

To use Mobile Device Management features for Android devices it is required that you provide an API key from Google. This API key is also required if you want to see device locations (using Google Maps) for Android and iOS devices in the "Locate Mobile Device View" of Endpoint Protector.

4.2.1. What is GCM (Google Cloud Messaging) and why I need it?

In order to use the MDM features provided for Android a GCM API Key (Google Cloud Messaging for Android) is required. GCM is necessary to establish communication between an Android mobile device and Endpoint Protector and issuance to you is up to Google/Androids own discretion.

For more info about Google Cloud Messaging for Android, please refer to: http://developer.android.com/guide/google/gcm/index.html

For more info about Google Maps API, please refer to: https://developers.google.com/maps/

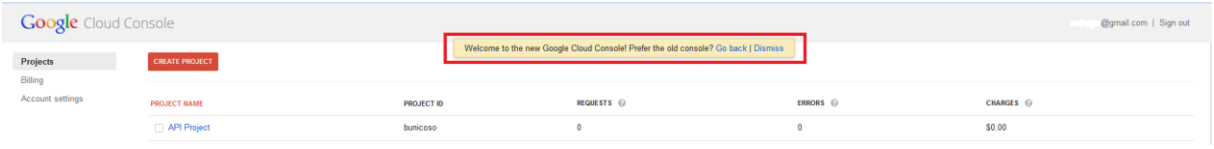
4.2.2. How to get your Google API Key for GCM and Maps?-new method (April 2014)

Visit the following site, Google Cloud Console, and login with your company Google account.

https://cloud.google.com/console

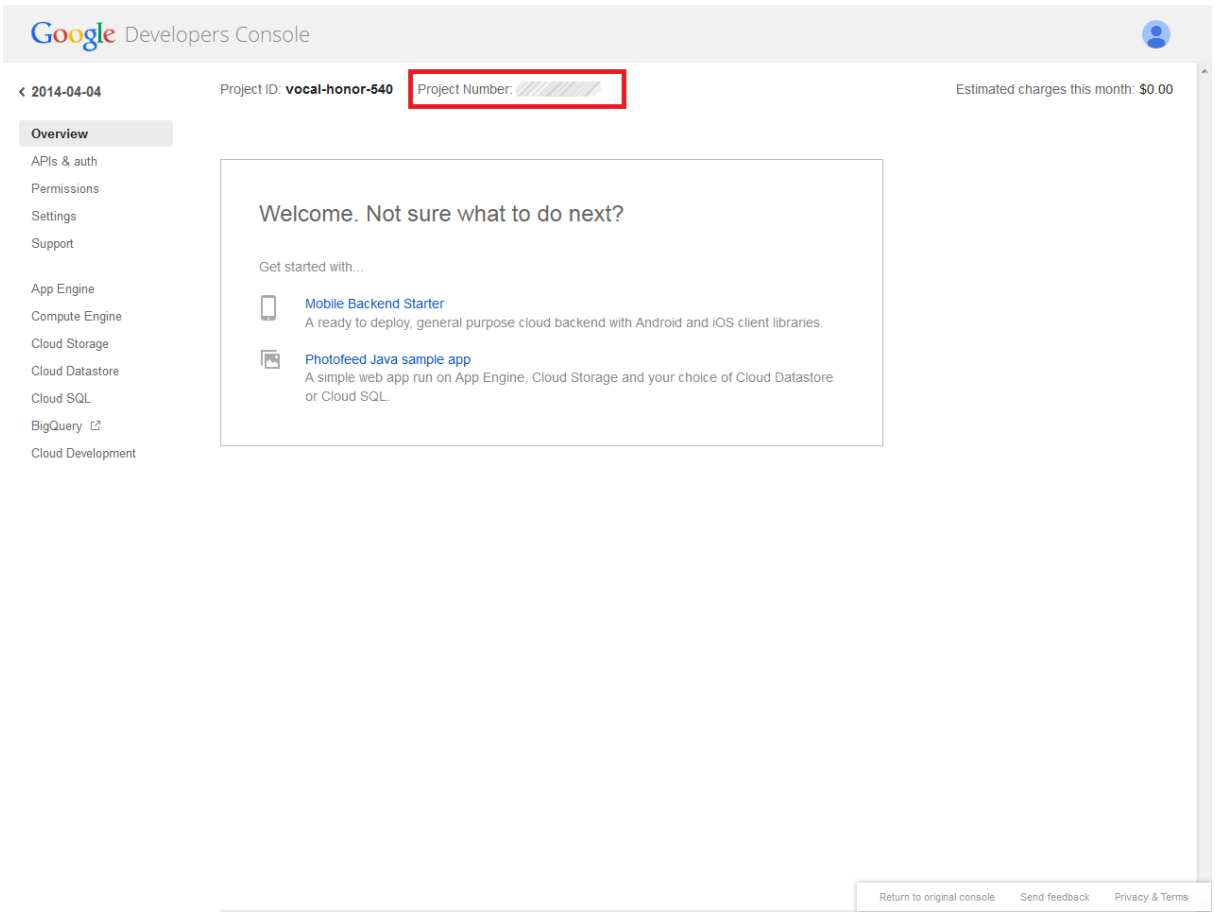
Note!

The old method can still be used by those who prefer it over the new. When you log in with your Google account to the console, you have the option to revert to the old style. To set up GCM with the old method, see paragraph 4.2.4 and 4.2.5.

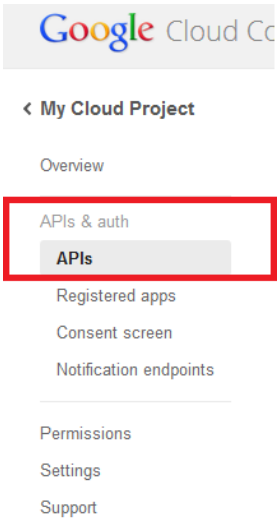


1. If you login to the Google Cloud Console for the first time you will be asked to "CREATE PROJECT". Select this option and give the project a name.

2. The Project will be given a Project Number by Google which you need to enter in the Endpoint Protector interface as described in the next paragraph.



3. In the left menu go to APIs & auth > APIs .

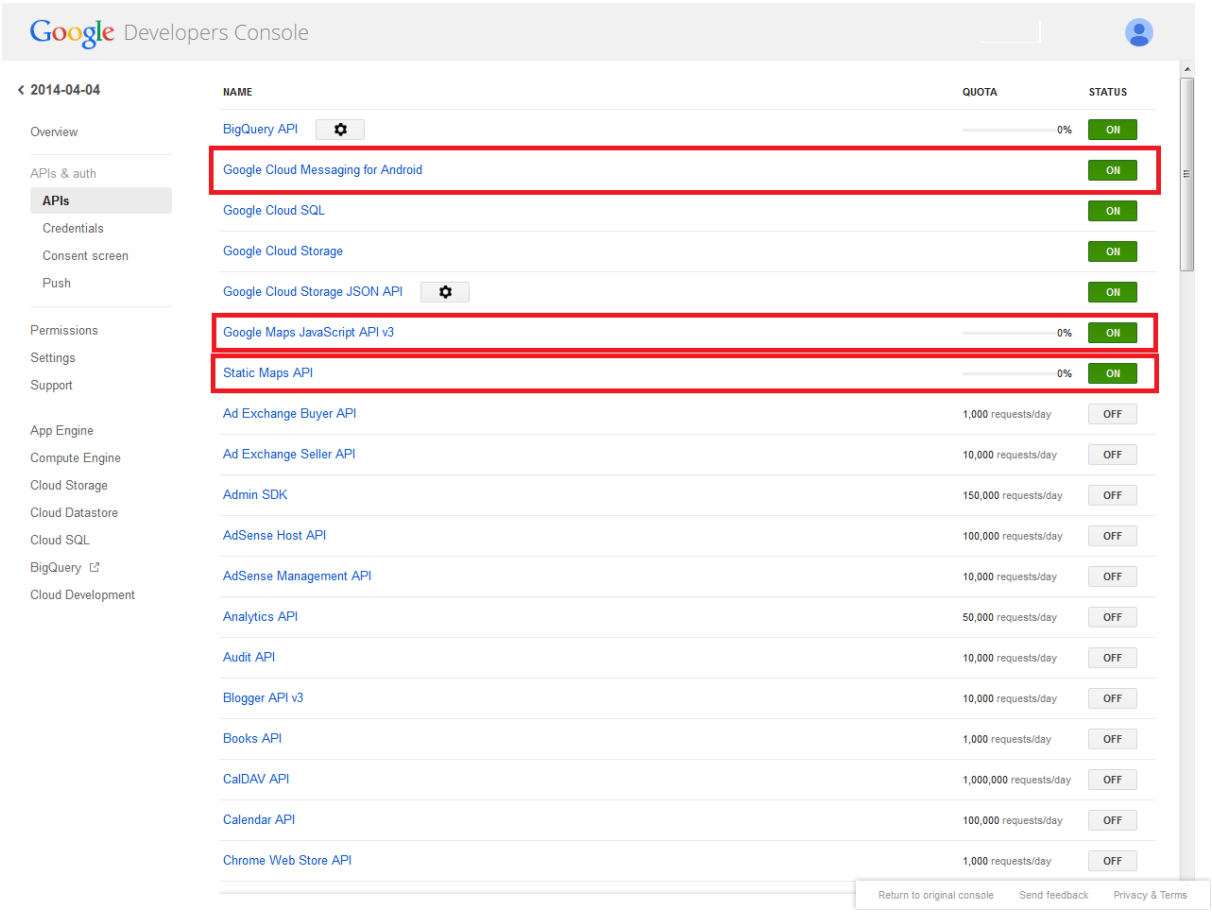


4. Make sure the following three Google Services have ON status (green):

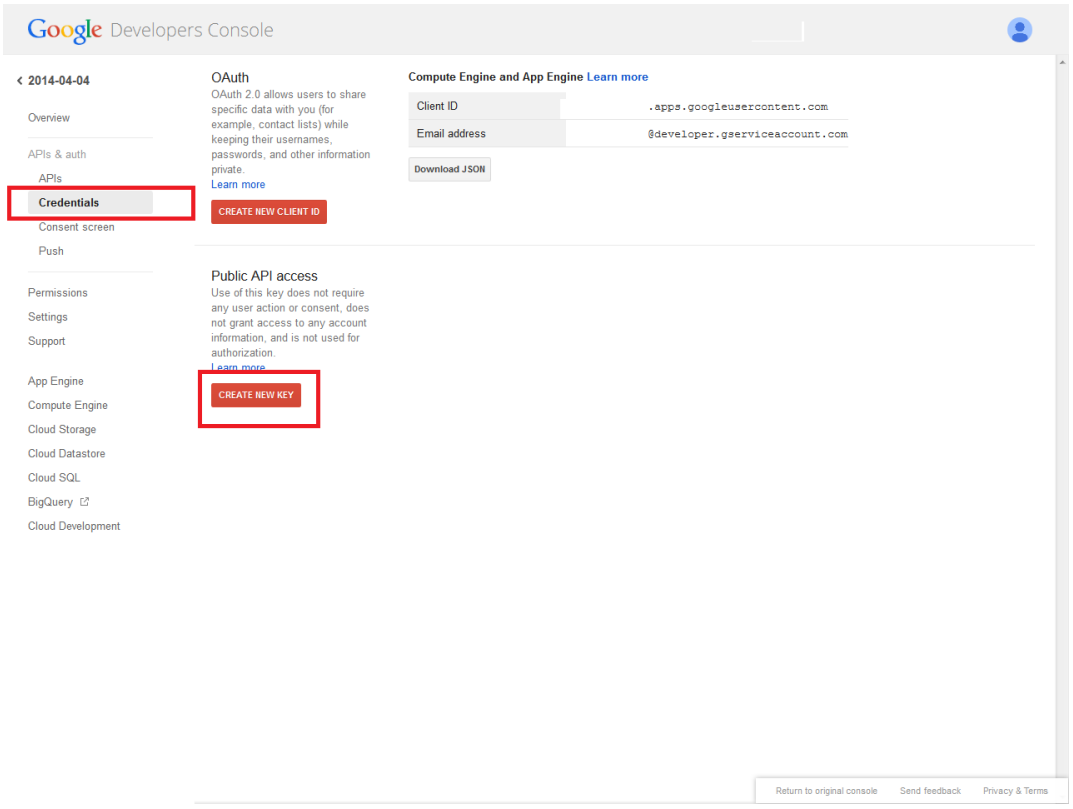
- **Google Cloud Messaging for Android,**

- **Google Maps JavaScript API v3,**
- **Static Maps API.**

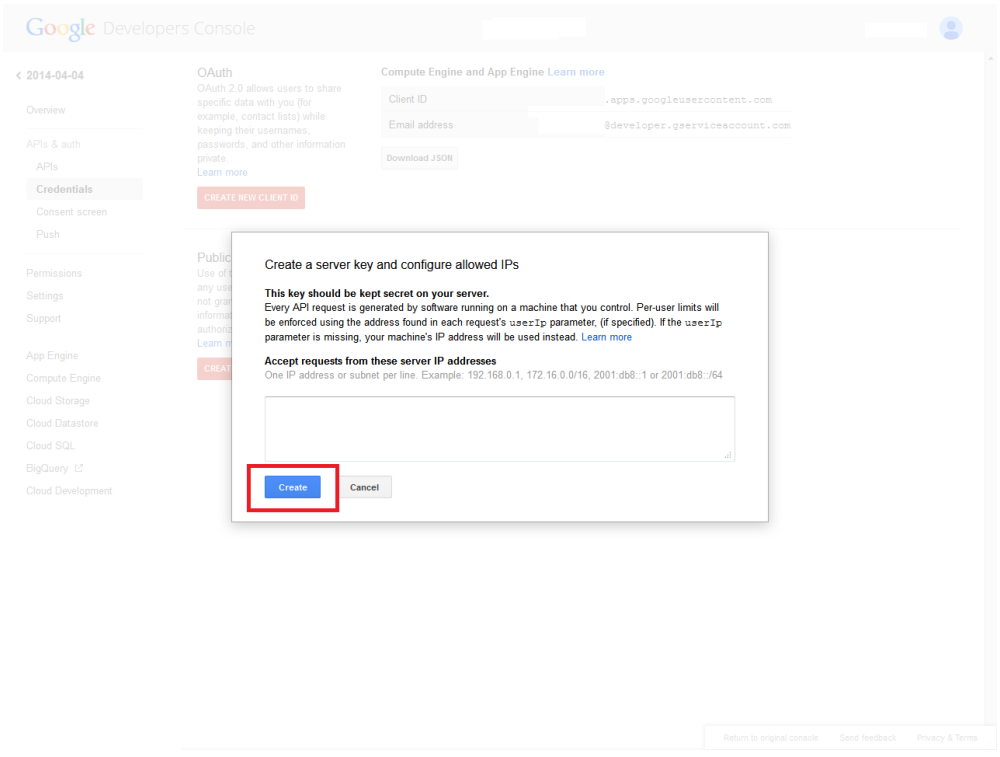
To enable these three services toggle it to the status ON.



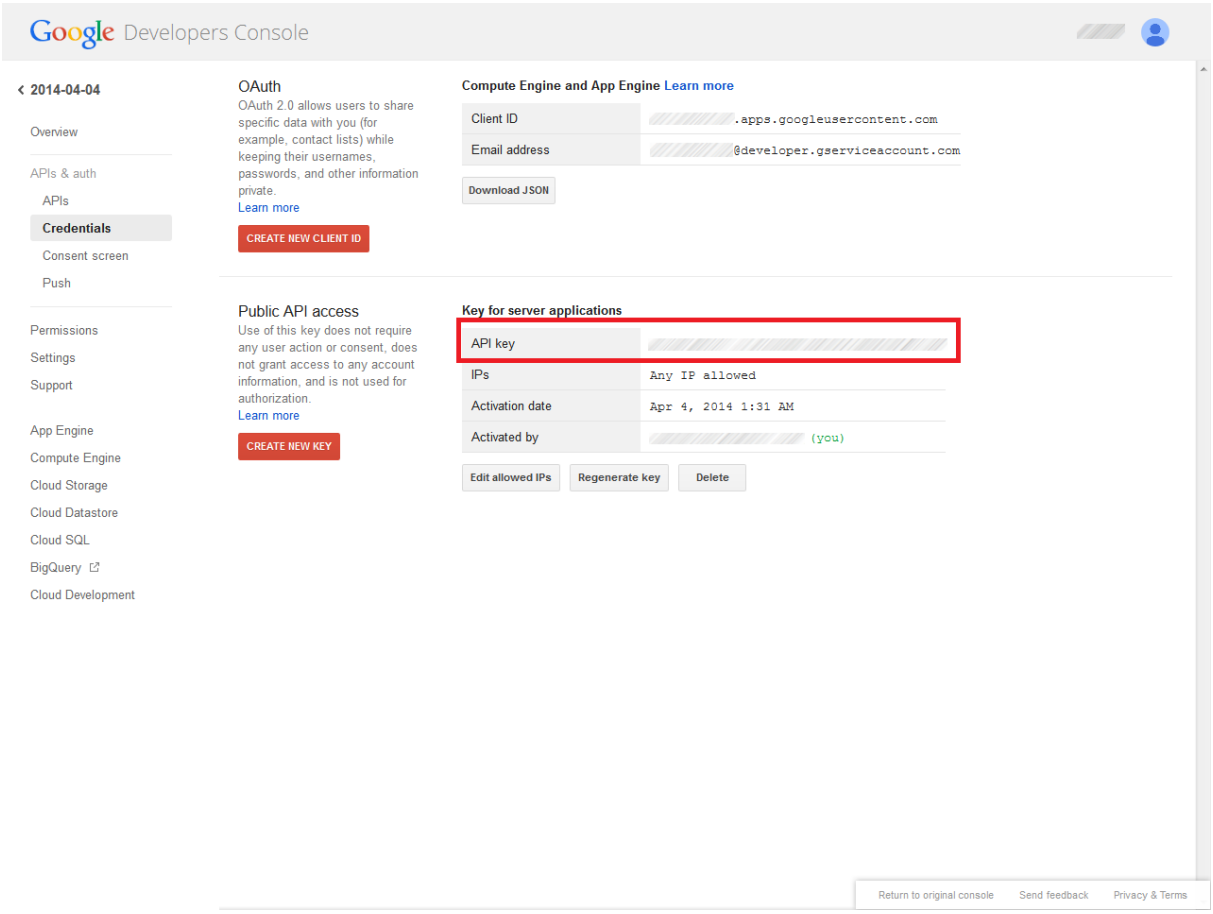
5. In the left menu go to Credentials. Create a new key. When prompted choose the Server key option.



6. Press Create, leaving the "Accept requests from these server IP addresses" field blank.


Google Developers Console
Create a server key and configure allowed IPs
This key should be kept secret on your server.
Every API request is generated by software running on a machine that you control. Per-user limits will be enforced using the address found in each request's userIp parameter, (if specified). If the userIp parameter is missing, your machine's IP address will be used instead. Learn more
Accept requests from these server IP addresses
One IP address or subnet per line. Example: 192.168.0.1, 172.16.0.0/16, 2001:db8::1 or 2001:db8::/64
Create
Cancel

7. You can now locate your API key under the "Key for server applications" section.
   The API key has the following format (Example API key):
   ExamplE67QWuu26-5j6WEEfWqgqYYouW1408-7



8. Copy the Google API key as described in the next paragraph in the Endpoint Protector interface.

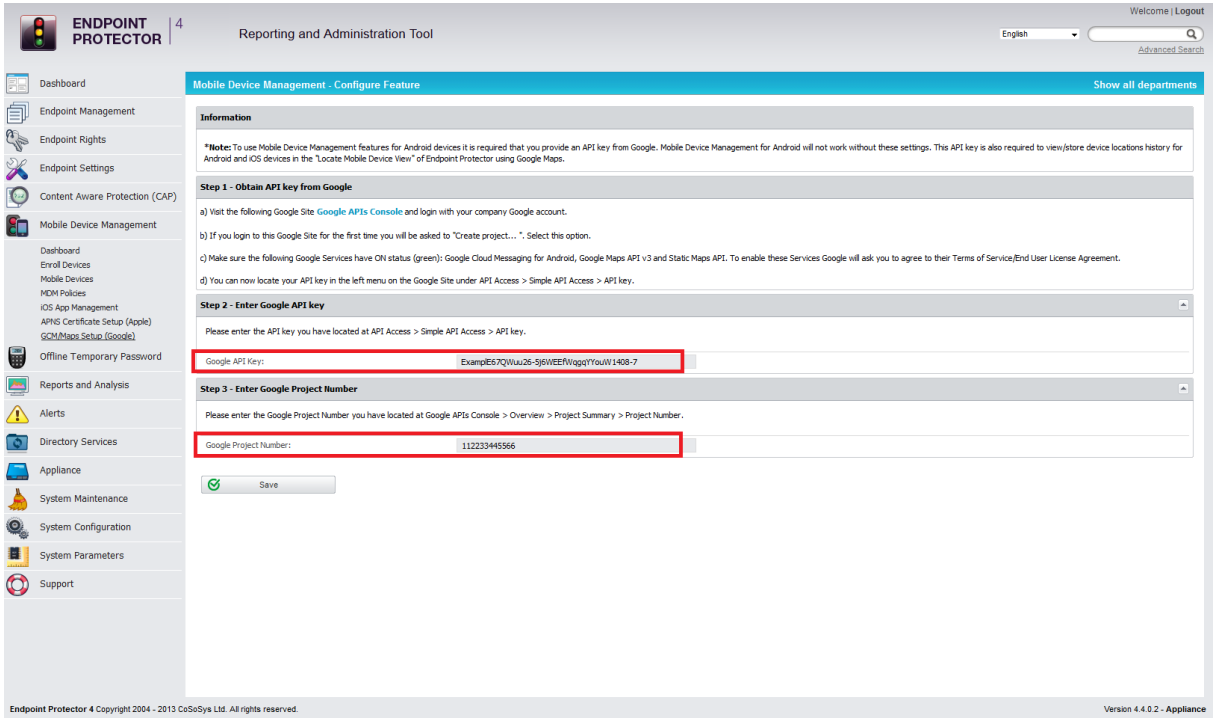
4.2.3. Entering Google API Key and Project Number in Endpoint Protector-new method

After you have obtained your Google API Key please enter it together with the Google Project Number in the Endpoint Protector Interface.

The Google Project Number you find on the Google Cloud Console Site under Projects > Overview > Project Number (paragraph 4.2.2, step 2).

The Server API Key you find on the Google Cloud Console Site under Projects > New Project> APIs & auth > Credentials > Key for server applications (paragraph 4.2.2, step 7).

Add them at Mobile Device Management > GCM/Maps Setup (Google).


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Dashboard
Enroll Devices
Mobile Devices
MDM Policies
iOS App Management
APNS Certificate Setup (Apple)
GCM/Maps Setup (Google)
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
System Configuration
System Parameters
Support
Mobile Device Management - Configure Feature
Show all departments
Information
*Note: To use Mobile Device Management features for Android devices it is required that you provide an API key from Google. Mobile Device Management for Android will not work without these settings. This API key is also required to view/store device locations history for Android and iOS devices in the "Locate Mobile Device View" of Endpoint Protector using Google Maps.
Step 1 - Obtain API key from Google
a) Visit the following Google Site Google APIs Console and login with your company Google account.
b) If you login to this Google Site for the first time you will be asked to "Create project... ". Select this option.
c) Make sure the following Google Services have ON status (green): Google Cloud Messaging for Android, Google Maps API v3 and Static Maps API. To enable these Services Google will ask you to agree to their Terms of Service/End User License Agreement.
d) You can now locate your API key in the left menu on the Google Site under API Access > Simple API Access > API key.
Step 2 - Enter Google API key
Please enter the API key you have located at API Access > Simple API Access > API key.
Google API Key:
ExamplE67QWuu26-5j6WEEfWqgqYYouW1408-7
Step 3 - Enter Google Project Number
Please enter the Google Project Number you have located at Google APIs Console > Overview > Project Summary > Project Number.
Google Project Number:
112233445566
Save
Endpoint Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved.
Version 4.4.0.2 - Appliance

After entering/copying the API Key and the Google Project Number press the "Save" button.

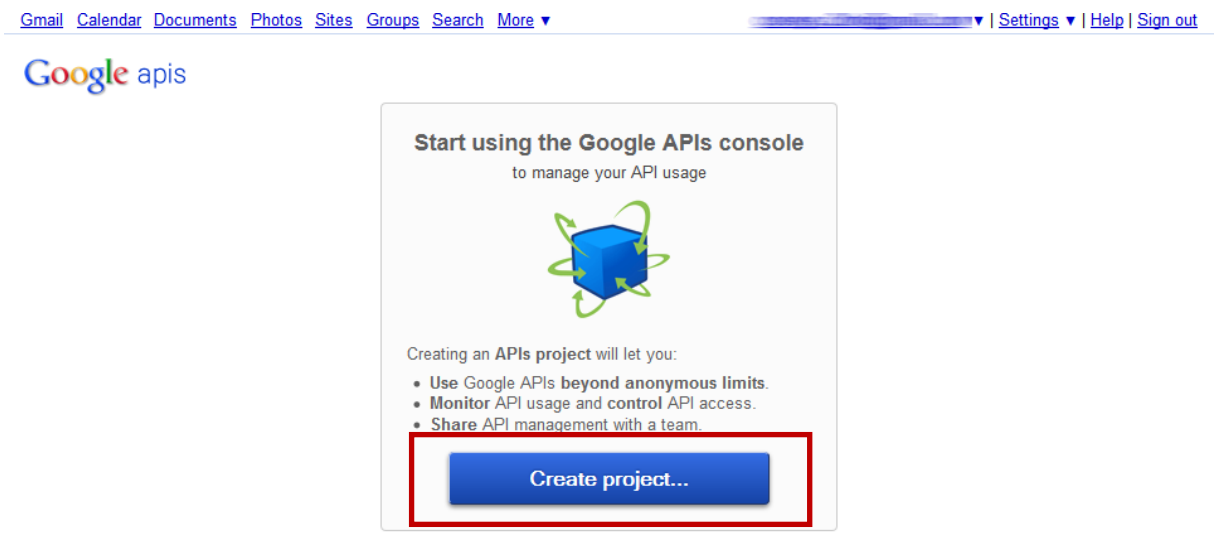
Once these steps were completed you can start enrolling Android devices to Endpoint Protector Mobile Device Management.

4.2.4. How to get your Google API Key for GCM and Maps?-old method

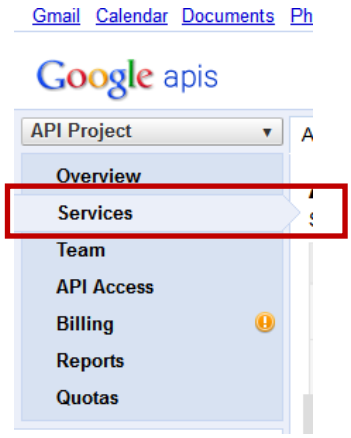
Visit the following Google Site Google APIs Console and login with your company Google account.

http://code.google.com/apis/console

1. If you login to the Google APIs Console for the first time you will be asked to "Create project…". Select this option and give the project a name. The Project will be given a Project Number by Google which you also need to enter in the Endpoint Protector interface as described in the next paragraph).


Gmail Calendar Documents Photos Sites Groups Search More ▾
▾ | Settings ▾ | Help | Sign out
Google apis
Start using the Google APIs console
to manage your API usage
Creating an APIs project will let you:
Use Google APIs beyond anonymous limits.
Monitor API usage and control API access.
Share API management with a team.
Create project...

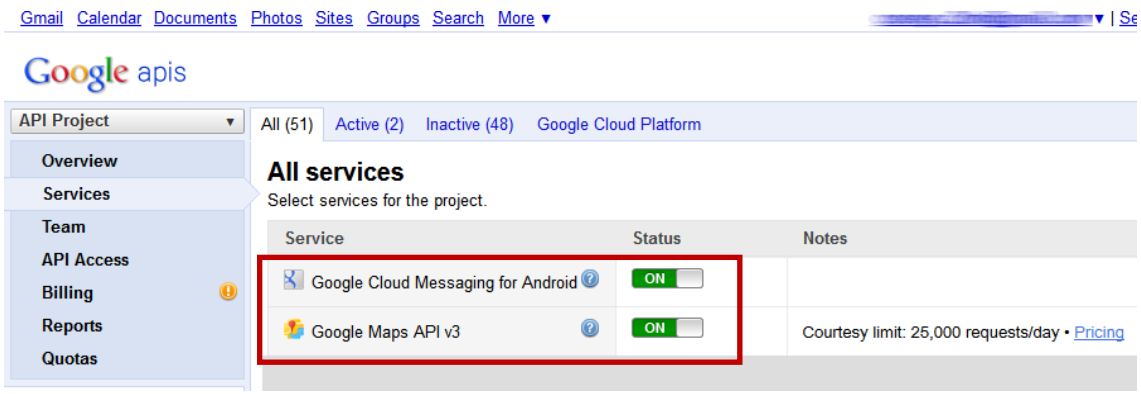
2. In the left menu on the Google APIs Console Site go to Services.



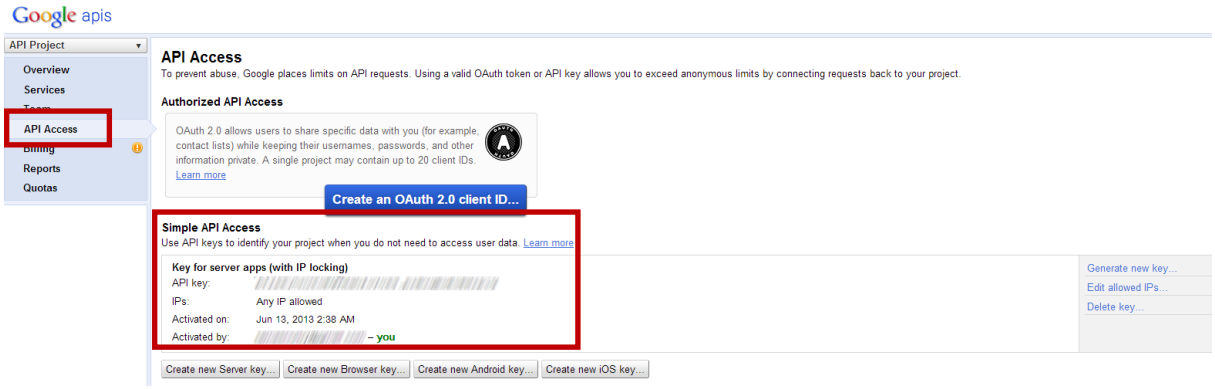
3. Make sure the following two Google Services have ON status (green):

- **Google Cloud Messaging for Android,**
- **Google Maps API v3.**

To enable these two services toggle it to the status ON, Google will ask you to agree to their Terms of Service/End User License Agreement.



4. You can now locate your API key in the left menu on the Google APIs Console Site under API Access > Simple API Access > API key.
   The API key has the following format (Example API key):
   ExamplE67QWuu26-5j6WEEfWqgqYYouW1408-7


Google apis
API Project
Overview
Services
API Access
Reports
Quotas
API Access
To prevent abuse, Google places limits on API requests. Using a valid OAuth token or API key allows you to exceed anonymous limits by connecting requests back to your project.
Authorized API Access
OAuth 2.0 allows users to share specific data with you (for example, contact lists) while keeping their usernames, passwords, and other information private. A single project may contain up to 20 client IDs.
Learn more
Create an OAuth 2.0 client ID...
Simple API Access
Use API keys to identify your project when you do not need to access user data. Learn more
Key for server apps (with IP locking)
API key:
IPs: Any IP allowed
Activated on: Jun 13, 2013 2:38 AM
Activated by: – you
Generate new key...
Edit allowed IPs...
Delete key...
Create new Server key...
Create new Browser key...
Create new Android key...
Create new iOS key...

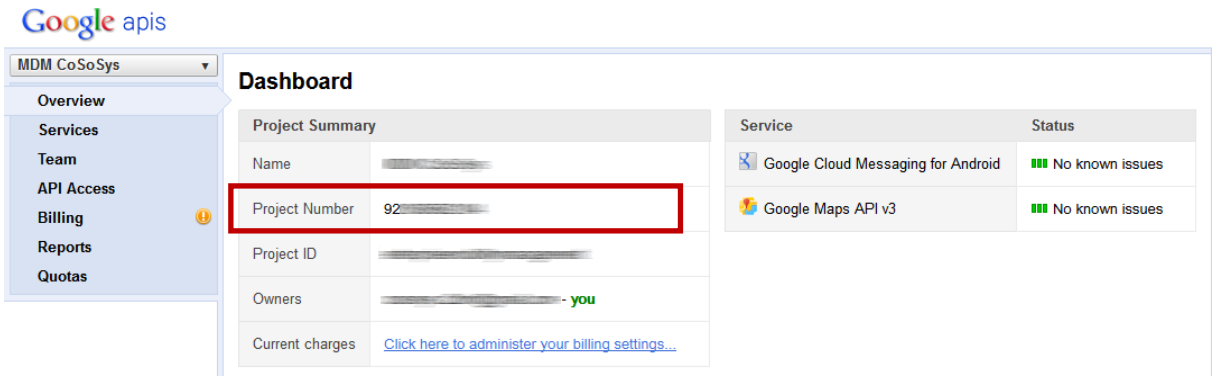
5. On the Google APIs Console Site in API Access > Simple API Access > you can also add referrers that are allowed to use your API keys, and we recommend you to add the following two. Do this by clicking on the right side next to the API key on "Edit allowed referrers…" and add there in separate lines:
   cloud.endpointprotector.com
   endpointprotector.com

6. Copy the Google API key as described in the next step in the Endpoint Protector interface.

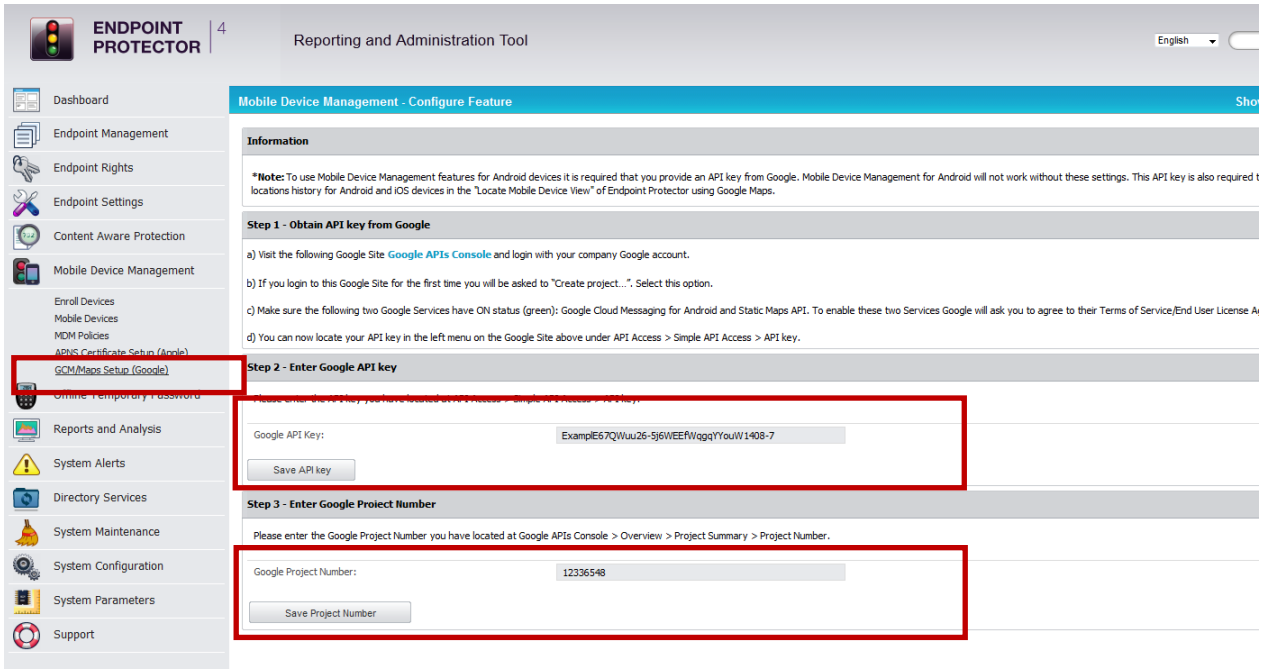
4.2.5. Entering Google API Key and Project Number in Endpoint Protector-old method

After you have obtained your Google API Key please enter it together with the Google Project Number in the Endpoint Protector Interface.

The Google Project Number you find on the Google APIs Console Site under > Overview > Project Number.



Add them at Mobile Device Management > GCM/Maps Setup (Google).


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
English
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection
Mobile Device Management
Enroll Devices
Mobile Devices
MDM Policies
APNS Certificate Setup (Apple)
GCM/Maps Setup (Google)
Reports and Analysis
System Alerts
Directory Services
System Maintenance
System Configuration
System Parameters
Support
Mobile Device Management - Configure Feature
Information
*Note: To use Mobile Device Management features for Android devices it is required that you provide an API key from Google. Mobile Device Management for Android will not work without these settings. This API key is also required t
locations history for Android and iOS devices in the "Locate Mobile Device View" of Endpoint Protector using Google Maps.
Step 1 - Obtain API key from Google
a) Visit the following Google Site Google APIs Console and login with your company Google account.
b) If you login to this Google Site for the first time you will be asked to "Create project...". Select this option.
c) Make sure the following two Google Services have ON status (green): Google Cloud Messaging for Android and Static Maps API. To enable these two Services Google will ask you to agree to their Terms of Service/End User License A
d) You can now locate your API key in the left menu on the Google Site above under API Access > Simple API Access > API key.
Step 2 - Enter Google API key
Google API Key:
ExamplE67QWuu26-5j6WEEfWqgqYYouW1408-7
Save API key
Step 3 - Enter Google Project Number
Please enter the Google Project Number you have located at Google APIs Console > Overview > Project Summary > Project Number.
Google Project Number:
12336548
Save Project Number

After entering/copying the API Key click "Save API Key".

Now enter the Google Project Number and click "Save Project Number".

After completing these steps you can start enrolling Android devices to Endpoint Protector Mobile Device Management.

4.2.6. Google C2DM

C2DM for Android is not supported by Endpoint Protector anymore.

5. iOS EPP MDM App

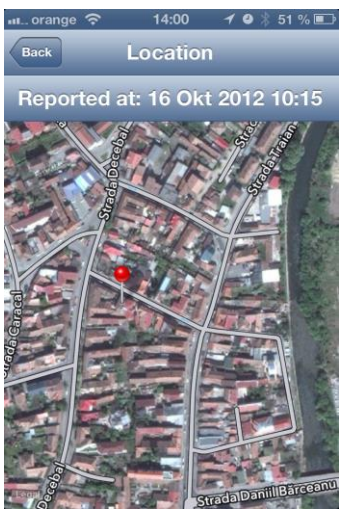
The EPP MDM iOS app is a free app for iOS available on the Apple App Store. The EPP MDM app is compatible with iPhone and iPad. It is an optional app and not a necessity for use of Endpoint Protector MDM for iOS. The EPP MDM app has two functions, one to locate the device and second to use the app optionally also as a way to enroll an iOS device to Endpoint Protector Mobile Device Management.

5.1. EPP MDM iOS App Supported iOS Versions

The EPP MDM app for iOS supports iOS version 7.0, 6.0, 5.0. iOS version 4.0 is not supported by the EPP MDM iOS app due to missing support for required features.

5.2. EPP MDM iOS App to locate devices

The EPP MDM app allows the iOS device to provide location data of the device to the Endpoint Protector Appliance in order to determine the current location of an iOS device in case it is misplaced, lost or stolen. To locate an iOS device the EPP MDM app is a necessity on the iOS device.



5.3. EPP MDM iOS App to enroll devices (optional)

The EPP MDM App allows the iOS device to enroll as described below at "iOS Mobile Device Enrollment through EPP MDM App". The EPP MDM App is not required for enrollment, it is simply an option to enroll in this way a device to Endpoint Protector Server.

5.4. EPP MDM iOS App Device Information

The EPP MDM app also detects device details and if a device was tampered with (Jailbreak Status).

5.5. Installing the EPP MDM iOS App

The EPP MDM app for iOS is available on the Apple App Store here:

https://itunes.apple.com/us/app/epp-mdm/id570954584?mt=8

Downloading and installing the application can be made directly on the iOS device by accessing App Store on the device, and entering EPP MDM in the search bar. The search result will show you EPP MDM by CoSoSys.

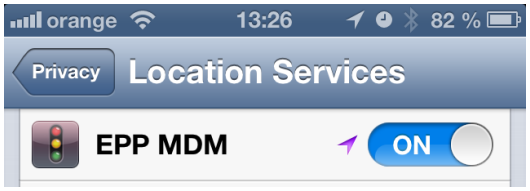
Click on the button "FREE" followed by "INSTALL APP". After that the EPP MDM app will be downloaded and installed on your device.

To start the EPP MDM app simply locate it on your iOS device home screen and click to start it.

5.6. Allow Location Services for EPP MDM iOS App

After starting the EPP MDM iOS app the user will be asked "EPP MDM would like to use your current location". The user has to select "OK" to allow Location Services. If this setting is not made correctly to allow the iOS EPP MDM app will not be able to report location information.

This setting can be checked on the iOS device in the following location:
iOS device home screen > Settings > Privacy > Location Services
Location Services have to be set to "ON" and for the EPP MDM set to "ON" as well. Next to the "ON" a small compass needle icon is shown as well.



5.7. Pushing and Managing EPP MDM App to iOS Devices

The EPP MDM App can be pushed and managed to any supported and managed iOS device.

For details how to push the EPP MDM App to an iOS devices check section 12.4 (Pushing Apps to iOS Devices).

6. Android Endpoint Protector MDM Client App

The Android **Endpoint Protector MDM Client** app is a free app for Android and available on the Google Play Marketplace here:

https://play.google.com/store/apps/details?id=com.cososys.eppclient&hl=en

The Android EPP Client app is MANDATORY for use of Endpoint Protector MDM with Android devices.

6.1. EPP MDM Android Client App Supported Versions

The EPP MDM app for Android is compatible with Android devices using Android Version 2.2 (Codename Froyo) or newer.

6.2. The Android EPP Client App

The Android EPP Client app allows the Android device to provide Endpoint Protector MDM with management rights. It also offers location data of the device to the Endpoint Protector Appliance in order to determine the current location of an Android device in case it is misplaced, lost or stolen.

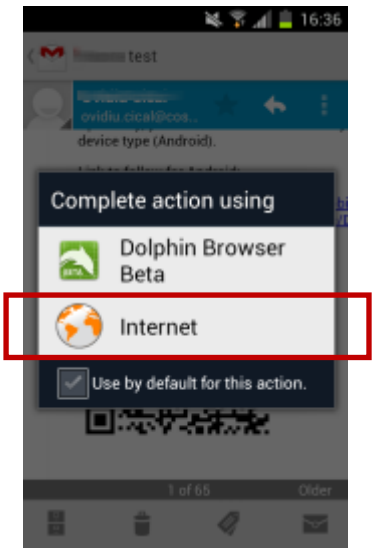
6.3. EPP Client Android App to enroll devices

The Android EPP Client App is required for enrollment of an Android mobile device to an Endpoint Protector Appliance.

6.4. Install EPP Client App on Android and Enrolling Android Device

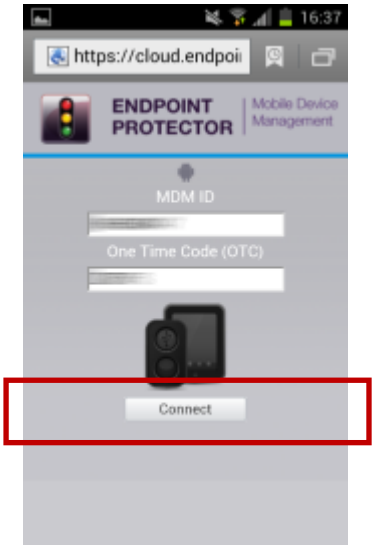
After receiving the enrollment invitation E-Mail or SMS click on the link provided in the E-Mail or SMS.

1. Choose to open the link with the default browser on your Android device.



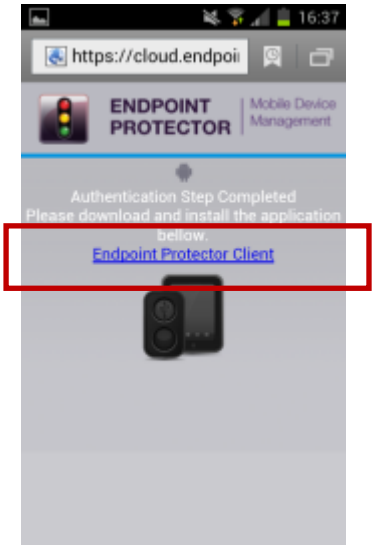
In this case (screenshot above) the choice for native browser is the option "Internet", not the Dolphin or any other browser that might be installed on your Android device.

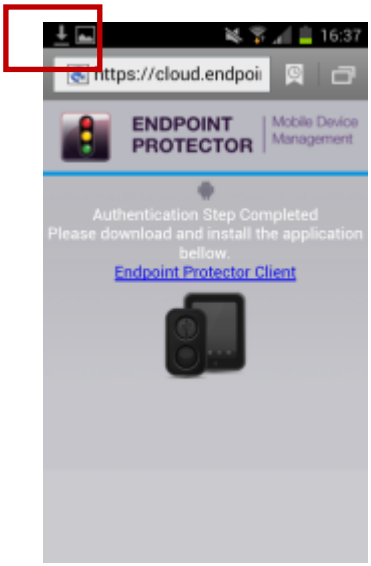
2. The web browser will open the enrollment site that already includes your registration data consisting of an MDM ID and your One Time Code (OTC).



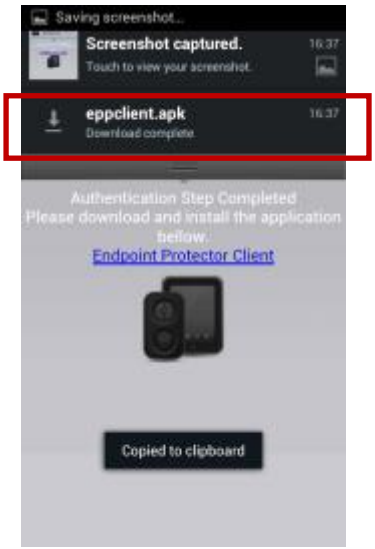
Click "Connect" to proceed"

3. In the next step the device user has to click on the "Endpoint Protector Client" link. Then a download of the EPP Client App will start.

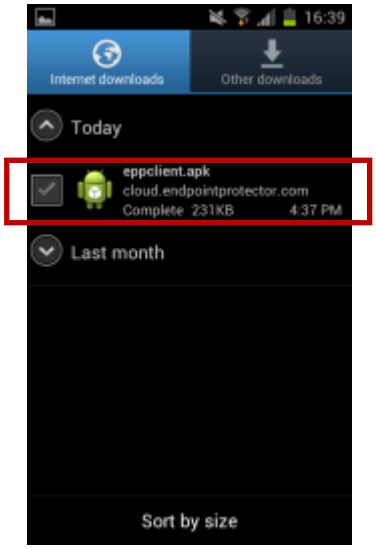




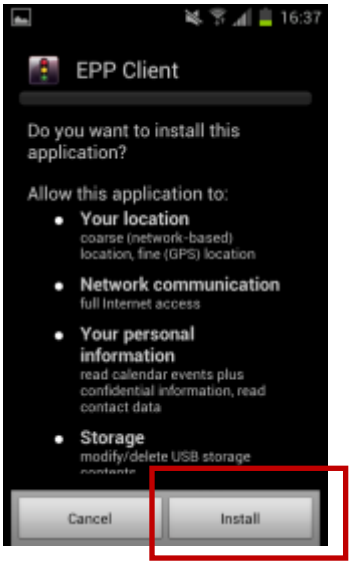
4. The download of the eppclient.apk (name of the EPP Client Android app download file) should finish rather fast depending on your data connection speed since the eppclient.apk is small.

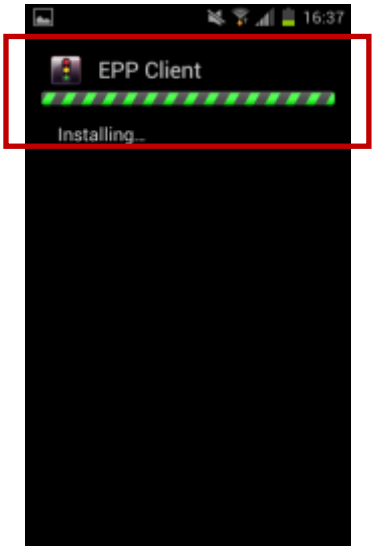


5. Locate now the eppclient.apk in the download folder on your device.

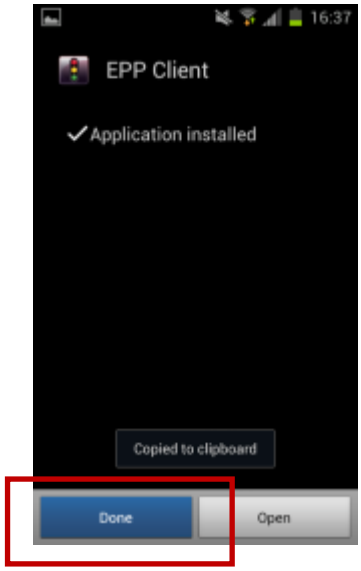


6. Click on the eppclient.apk and select "Install". The EPP Client will start to install itself on the Android device.

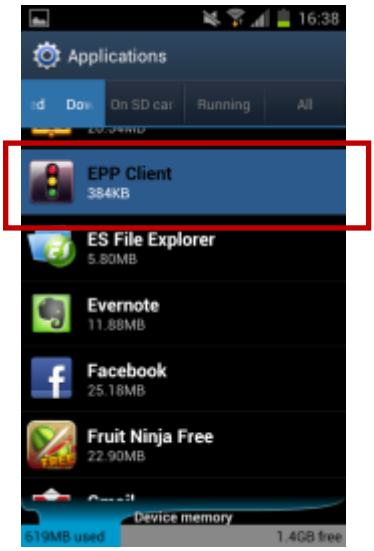




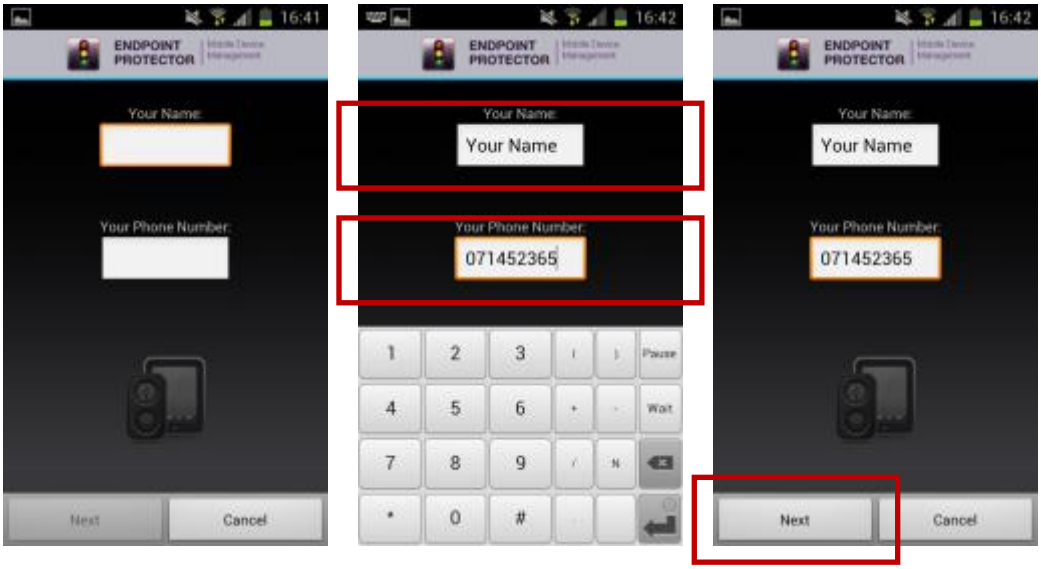
7. After the installation you will see a message indicating the installation is finished. Click "Done" to complete the final steps for your Android device enrollment.



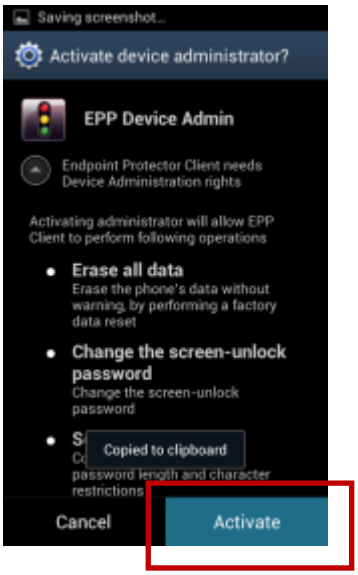
8. Go to "Applications" on your Android device. There locate the EPP Client and start it.



9. After the EPP Client starts you need to fill in your Name and your Phone Number. If the device has no phone number provide your mobile number for the Administrator to easier link your device with you as a user. Click "Next" after you completed the fields.



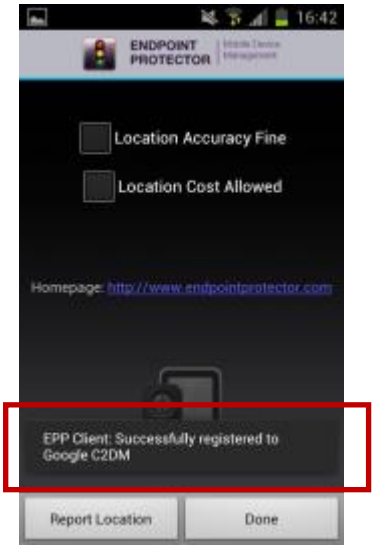
10. Now the question regarding device administration will appear which needs to be confirmed by clicking "Activate".


Saving screenshot...
Activate device administrator?
EPP Device Admin
Endpoint Protector Client needs Device Administration rights
Activating administrator will allow EPP Client to perform following operations
Erase all data
Erase the phone's data without warning, by performing a factory data reset
Change the screen-unlock password
Change the screen-unlock password
Copied to clipboard
password length and character restrictions
Cancel
Activate

Attention!

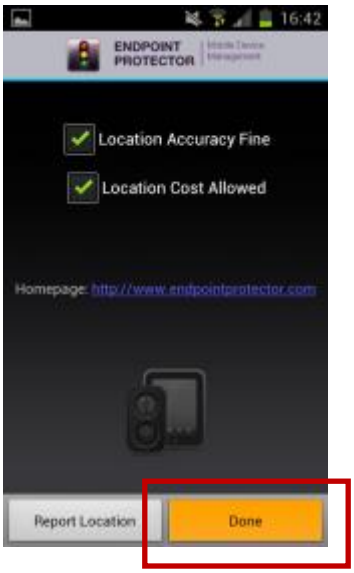
By not enabling this option, the Android mobile device cannot be remotely administrated / managed.

11. Now you will see the message "EPP Client Successfully registered to Google GCM or C2DM". This means that your Android device is now enrolled.



12. The settings "Location Accuracy Fine" or "Location Cost Allowed" can be selected.

    Click "Done" to finish the enrollment process.



    These two settings are described in the chapter 11.6.1 Location Accuracy Fine on Android 11.6.2 Location Cost Allowed on Android.

7. Enrolling Mobile Devices

Enrolling Mobile Devices means to establish the connection for communication and management between the Endpoint Protector Appliance and your mobile devices. It is the process of inviting, enrolling and connecting the device with your Endpoint Protector Appliance.

To enroll mobile devices it is required to have the setup for either APNS (for iOS and OS X) or GCM (for Android) as described in chapter 4. MDM Setup APNS (Apple) & GCM finalized. If the Setup for APNS or GCM is not finalized the Endpoint Protector Appliance will not give you access to > Enroll Devices.

7.1. Different Enrollment methods are available:

A mobile device can be enrolled by:

1. Accessing a link in the invitation E-mail send to the device
2. Scanning a QR code contained in the invitation E-mail for a device
3. Accessing a link contained in the invitation SMS send to the device
4. Accessing directly a link through the native web-browser on the device and completing the Endpoint Protector ID and OTC fields
    a. For iOS devices the link is: https://cloud.endpointprotector.com/mobile.php/register/iOS
    b. For OS X devices the link is:

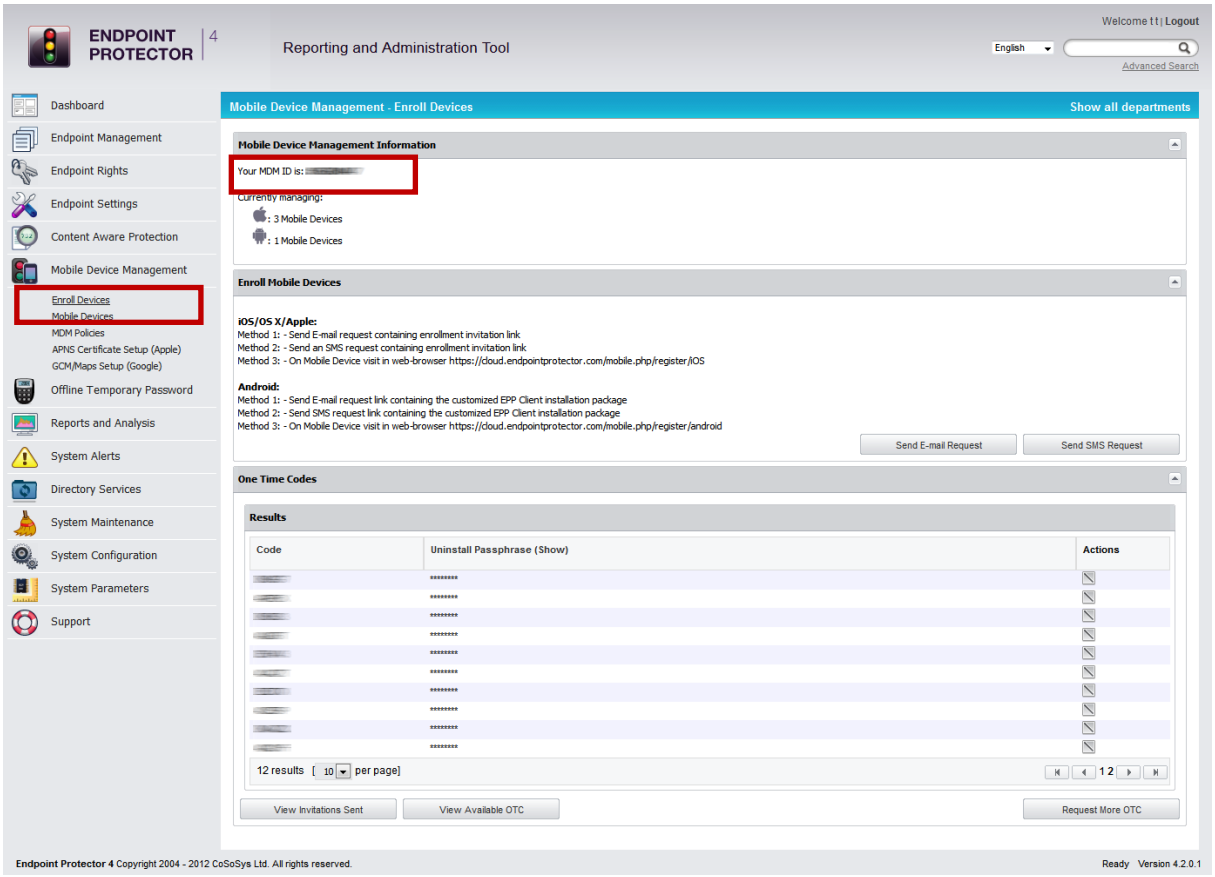
    https://cloud.endpointprotector.com/mobile.php/register/OSX

    c. For Android devices the link is: https://cloud.endpointprotector.com/mobile.php/register/android
5. Downloading and installing the EPP MDM app on an iOS, OS X or Android device and completing the Endpoint Protector ID and OTC fields

Attention!
Enrollment of iOS and OS X devices should be done through the Safari browser on your iOS and OS X device. Other browsers are not supported. For Android devices enrollment should be done through the native web browser on the device.

7.2. Mobile Device Enrollment

To be able to manage mobile phones and tablets, each device must be enrolled by going to Mobile Device Management -> Enroll Devices option.



In the Enrollment window, under Mobile Device Management Information, the MDM ID corresponding to your appliance is displayed, which will be further used as a parameter for enrolling mobile devices. Additionally, one can check the exact number of mobile devices enrolled at that moment.

The enrollment of iOS, OS X and Android devices is similar in many ways. There are different enrollment options for each mobile device type available. The first two options allow the sending of E-mail and SMS based invitation requests to mobile devices, invitations which include short instructions on the steps required for the end users of the device to perform. The sending of E-mail invitations can be performed by clicking on the "Send E-mail request" button, while the SMS based invitation can be performed by clicking on the "Send SMS Request" button. The "Bulk Enrollment" feature allows the administrator to send mass enrollment requests with just a few clicks. The administrator must create a contact list, either by pasting it into the contacts list field, or by importing it. After the contacts are added, either way, they will be shown in the interface, and with the "Add to sending queue" button the "Bulk Enrollment" process can be started and the invitations will be sent to all contacts (more on "Bulk Enrollment" at paragraph 7.2.10).

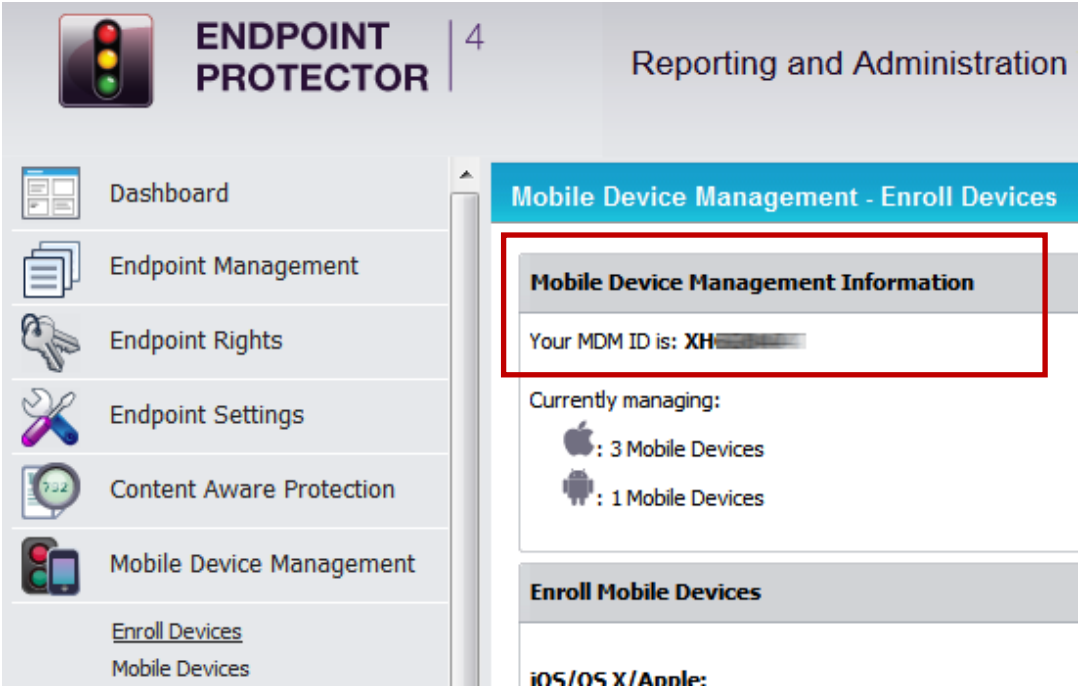
In order to ensure that a mobile device is properly and securely enrolled, there are two keys required during the enrollment process:

- **MDM ID** – which uniquely identifies your Endpoint Protector Appliance/Server.

- **OTC (One-Time-Code)** – which allows only the invited devices to be enrolled on your Endpoint Protector Appliance/Server. The OTC will expire after one use.

- **Uninstallation Passphrase (applies to iOS and OS X)** – which allows the device to be unmanaged / uninstalled. The uninstallation option for iOS and OS X has to be chosen at enrollment time.

The MDM ID can be found in the Reporting and Administration web interface at: Mobile Device Management > Enroll Devices > Mobile Device Management Information



These invitations, in case of an unknown device type and E-mail request, will include three different registration links for the different types of devices (iOS, OS X and Android), which readily include the MDM ID and OTC. In case of an unknown device type and SMS request, the invitations will include two different registration links for iOS and Android, which already holds the MDM ID and OTC.

While the MDM ID is used for all enrolled mobile devices, different OTCs must be used for enrolling each mobile device. The Mobile Device Management feature comes with 10 pre-generated OTCs available in the Enrollment window. The "Request More OTC" option will allow the Administrator to generate more OTCs.

Once an E-mail or SMS based invitation request is sent, an OTC will be automatically assigned to the user requesting the enrollment of his device and it will be automatically removed from the list of available One Time Codes. To verify which OTC was assigned to each device and user, the administrator can click on the "View Sent Invitations" button, which will displayed a list of all used OTCs with the corresponding e-mail addresses and/or phone numbers where they were sent to. The "View Available OTC" allows the administrator to return to the list of unassigned OTCs.

The third enrollment method allows the end user to directly enroll his mobile phone through the Endpoint Protector Cloud Service, which can be accessed at two separate links, one for each supported mobile device operating system. This option requires the user to previously receive the MDM ID and OTC keys from the administrator. In this case, the administrator must reserve one OTC from the list for the user making the request either by:

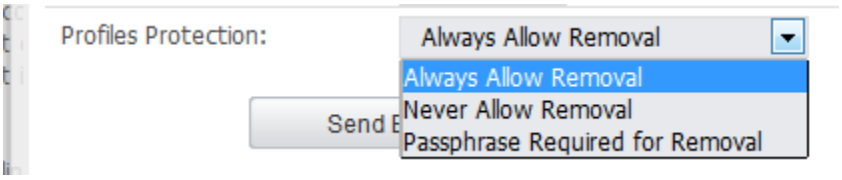
- using the "Reserve" right-click menu option

This operation will remove the selected OTC from the list of the available OTCs and move it to the list of already sent invitations.

7.2.1. iOS and OS X Enrollment and Profile Protection

When an iOS or OS X device is enrolled the Administrator has the option to protect the policy/settings (called Profiles on iOS and OS X) against uninstallation. When an iOS or OS X device is enrolled it receives first an enrollment profile which is responsible for the communication between the device and the Endpoint Protector Appliance. This enrollment profile is not protected against uninstallation but all additional profiles attached to the enrollment profile can be protected against uninstallation. This means the restriction profile cannot be uninstalled from the device without a passcode that is protecting it, but the enrollment profile can be uninstalled, which also will uninstall the restriction profile.

The Profile Protection options are:



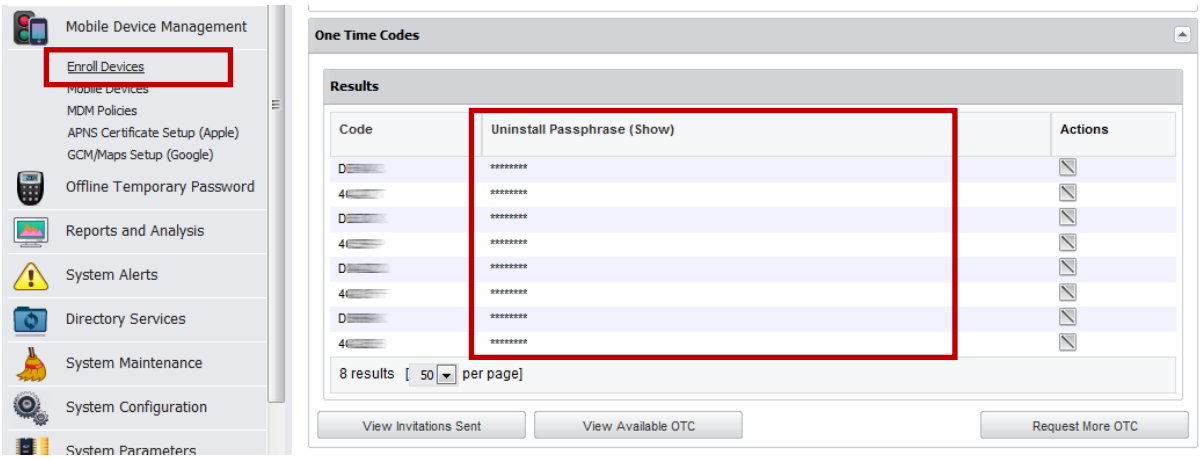
- **Always Allow Removal** – which allows the user to remove a profile at any time.
- **Never Allow Removal** – which allows removal of the profiles only through the Endpoint Protector Appliance Administrator.
- **Passphrase Required for Removal** – which allows the device user to delete the profile after entering the passphrase for deletion.

A practical example to illustrate this fact better is the following. An iPhone is enrolled and the administrator applies the companies' security policy for restrictions (disabling FaceTime for example) and WiFi Settings as a profile and protects it with a profile protection. The user of the device wants to uninstall the restrictions profile to be able to use FaceTime. To do that the user is required to enter a passcode which he doesn't know (only the Endpoint Protector administrators). The user still could uninstall the enrollment profile (without a passcode) but in case he does that also all his other profiles and settings are deleted along with it, meaning company WiFi settings etc.

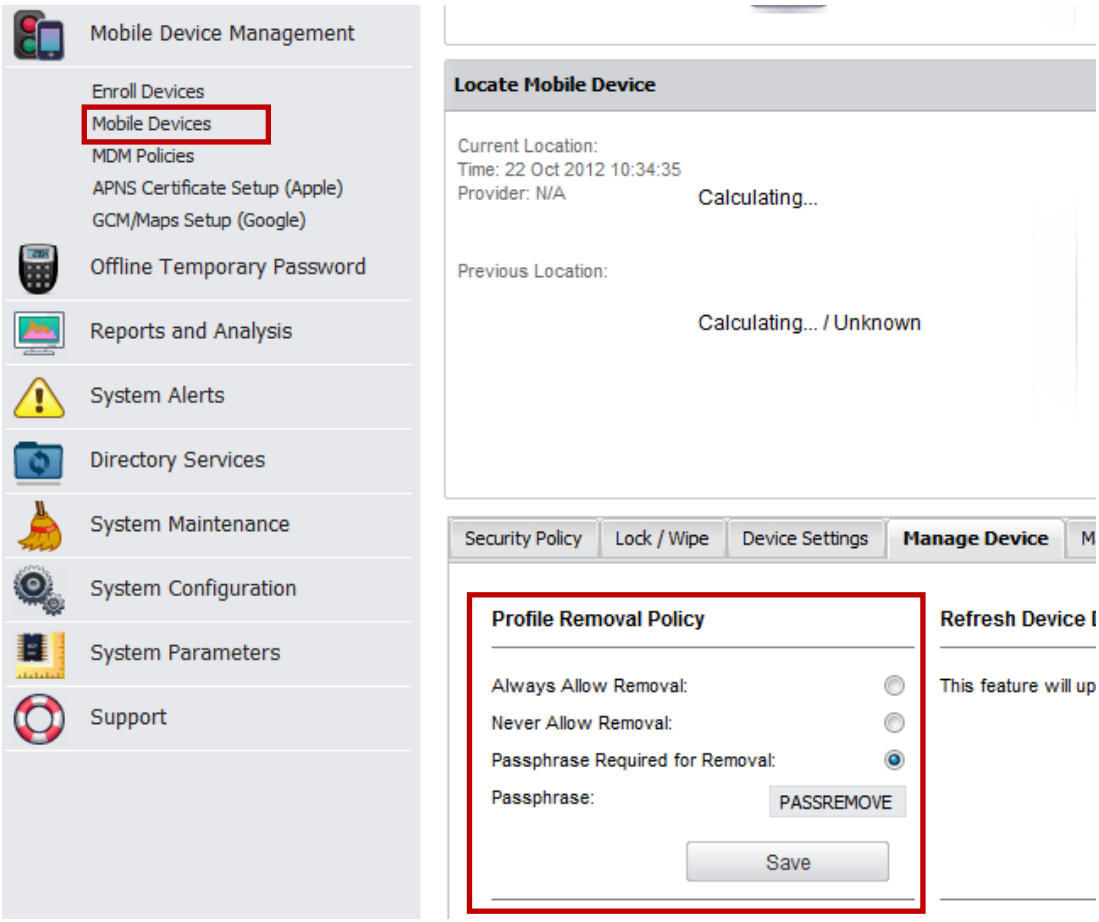
7.2.2. iOS and OS X Profile Protection Deletion Passphrase

The passphrase for deletion of Profiles on iOS and OS X devices is by default generated randomly if during the invitation/enrollment process the Endpoint Protector Administrator who sends the invitation to the device sets the Profile Protection option to “Passphrase Required for Removal”.

The automatically generated passphrase can be found in the Endpoint Protector Reporting and Administration web interface under
Mobile Device Management > Enroll Devices > One Time Codes > Uninstall Passphrase (show).
After clicking on show the Passphrase is shown that corresponds to the devices enrollment OTC. In case the device user needs this passphrase the administrator can give it to the user over the phone for the user to enter during deleting of a profile. The administrator can locate the Passphrase after clicking “View Invitations Sent” and locating the OTC used by the device for enrollment.

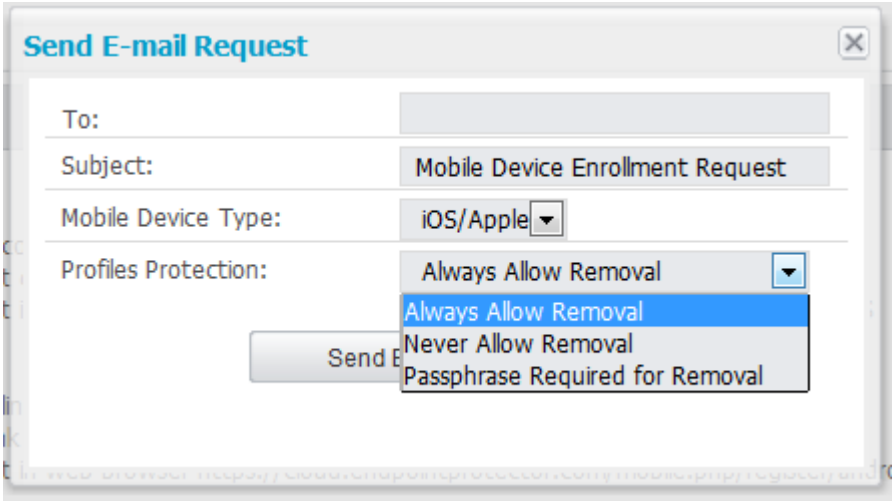


The Passphrase can also be set by the administrator manually under the option Mobile Device Management > Mobile Devices > Select Device > Manage Device > Profile Removal Policy



7.2.3. Sending E-Mail or SMS Enrollment Invitation (iOS/OS X / Android)

Sending E-Mail or SMS enrollment invitations is made through the option "Enroll Devices".



Entering E-Mail and Phone numbers require attention to the correct format and selecting the device type, if known, in this step is of advantage due to a lesser chance that the user will select the wrong option.

For iOS and OS X devices in the device enrollment step as previously described it is important to set the Profile Protection settings.

7.2.4. SMS Enrollment Number Format (iOS / Android)

When sending SMS enrollment invitations it is essential to send them using the correct number format.

The correct number format is: 401112345678

Country code, followed by area code and number, No + or zeroes are required in front of the country code.

At all-time a country code is required, in case of US or Canadian numbers it is a 1, for Germany it is 49, etc.

Note!

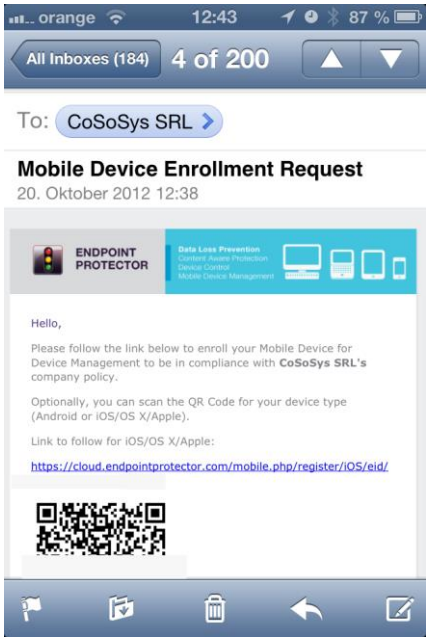
SMS Enrollment is not available for OS X !

7.2.5. E-Mail Enrollment Invitation (iOS/OS X / Android)

The device user can receive an enrollment invitation on the actual device and access the included URL (which includes already the MDM ID and OTC) to enroll the device.

Or if the e-mail is received with a desktop e-mail client, the user can scan the containing QR Code in the e-mail (which includes already the MDM ID and OTC) or access the included URL by typing it in the browser on the mobile device.

Below is shown an enrollment invitation e-mail on an iOS device.


orange
12:43
87 %
All Inboxes (184)
4 of 200
To:
CoSoSys SRL
Mobile Device Enrollment Request
20. Oktober 2012 12:38
ENDPOINT PROTECTOR
Hello,
Please follow the link below to enroll your Mobile Device for Device Management to be in compliance with CoSoSys SRL's company policy.
Optionally, you can scan the QR Code for your device type (Android or iOS/OS X/Apple).
Link to follow for iOS/OS X/Apple:
https://cloud.endpointprotector.com/mobile.php/register/iOS/eid/

In case the e-mail invitation is sent to an unknown device type it is important that the user chooses the proper device type from the available link options for iOS, OS X and Android devices.

7.2.6. SMS Enrollment Invitation (iOS / Android)

The device user should receive the enrollment invitation SMS on the actual device and access the included URL (which includes already the MDM ID and OTC) to enroll the device through the native browser of the device. In case of iOS it has to be accesses using Safari on the iPhone or iPad.

Below is shown an enrollment invitation SMS on an iOS device.

Note!

SMS Enrollment is not available for OS X!

7.2.7. iOS and OS X Mobile Device Enrollment over URL

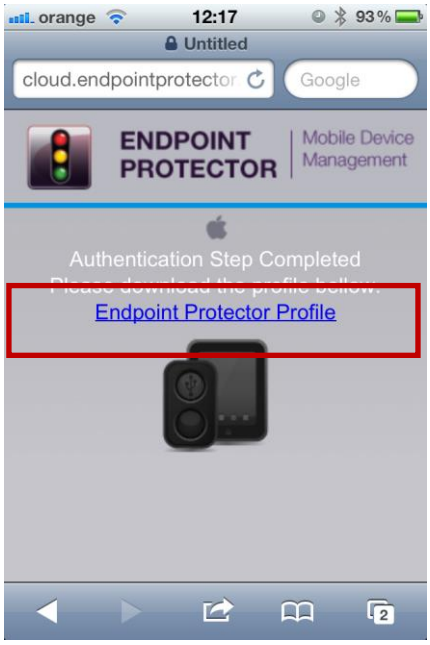
Attention!

Enrollment of iOS devices should be done through the Safari browser on your iOS device or the iOS EPP MDM app from the App Store. Using other web browsers to enroll your iOS device is not supported.

The enrollment of an iOS or OS X device requires a working Internet connection (Wi-Fi or 4G/3G/2G). A 3G data connection is recommended for mobile devices. This way the communication with the Apple Servers can be performed and the information about the mobile device can be further transmitted to the Endpoint Protector Appliance/Server.

Once the user has received the invitation and clicked on the included link, a confirmation page will be displayed in his browser, auto-filled with the MDM ID and OTC keys.

After clicking on the “Connect” button, the user receives an Endpoint Protector profile for download, which must be further installed on his mobile device.

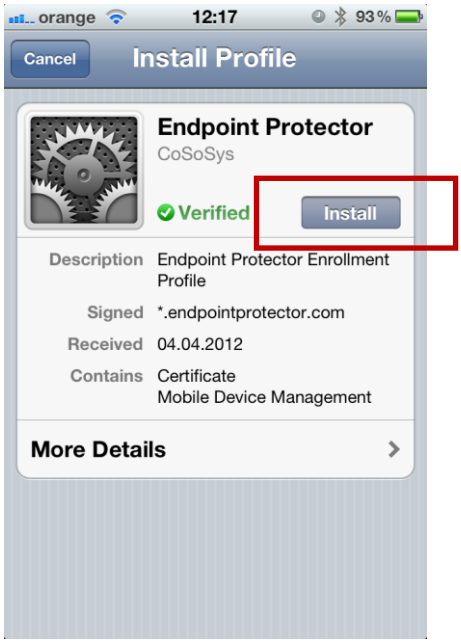


The user has to click on "Endpoint Protector Profile" to continue. The Profile has been generated at this step and is ready for installation.

Note!

The profile is valid from this point on for two (2) hours. If the enrollment process is at this point interrupted for more than two hours the enrollment process has to be repeated from the start.

Next, the user must click on the "Install" button for the installation of the Endpoint Protector Profile.

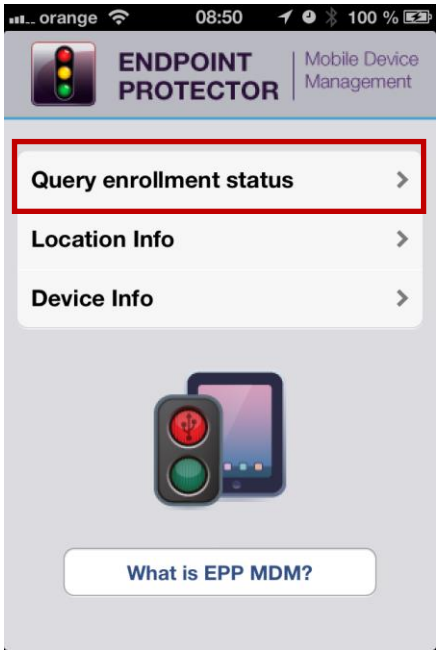


In case the iOS or OS X device has already a passcode/password set to access the device the user is asked to access the passcode/password in order to confirm installation.

Once the Endpoint Protector Profile was successfully installed, the mobile device will be displayed inside the Mobile Devices List from the Endpoint Protector Web based Reporting & Administration Interface and it now available for the administrator to manage it.

7.2.8. iOS Mobile Device Enrollment through EPP MDM App

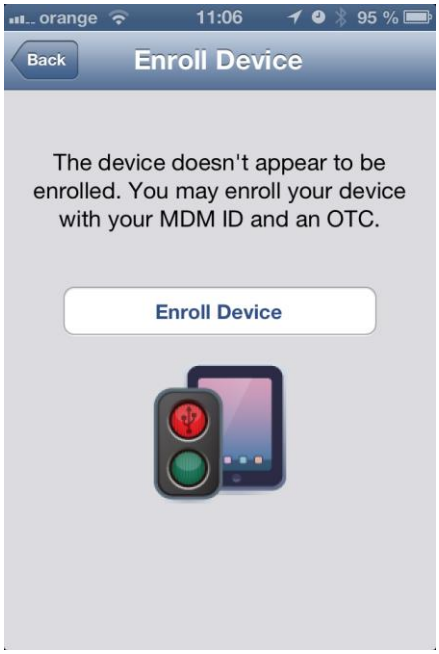
To enroll using the EPP MDM iOS app from the Apple App Store the user has to install the app on the iOS Device. After installing the EPP MDM iOS app (as described before in 5.5 Installing the EPP MDM iOS App) the user has to click "Query enrollment status"



The app is now checking if the iOS device is already enrolled with Endpoint Protector Mobile Device Management.

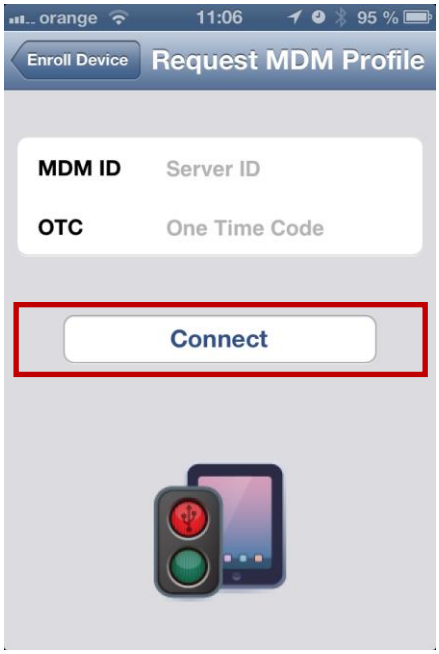
If the device is not enrolled yet the following message will appear "The device doesn't appear to be enrolled…." If the device is enrolled already it will appear

"Device enrolled".

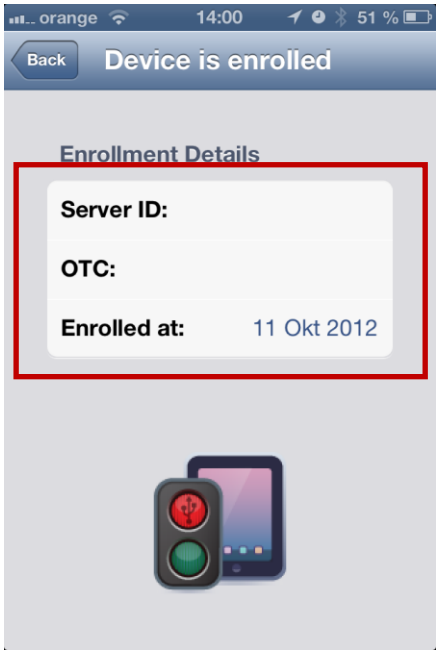

orange
11:06
95 %
Back
Enroll Device
The device doesn't appear to be enrolled. You may enroll your device with your MDM ID and an OTC.
Enroll Device

Left image, device not enrolled yet. *Right image, device is already enrolled.*

In case the device is not enrolled yet click "Enroll Device" to continue.



Provide the MDM ID (MDM ID is located as described before 7.2) and an OTC (One Time Code) that is provided by the Endpoint Protector Administrator and click "Connect".



After a device is successfully enrolled the Device enrolled status displays the MDM ID (Server ID) and OTC used along with the date when the device was enrolled.

7.2.9. Android Device Enrollment

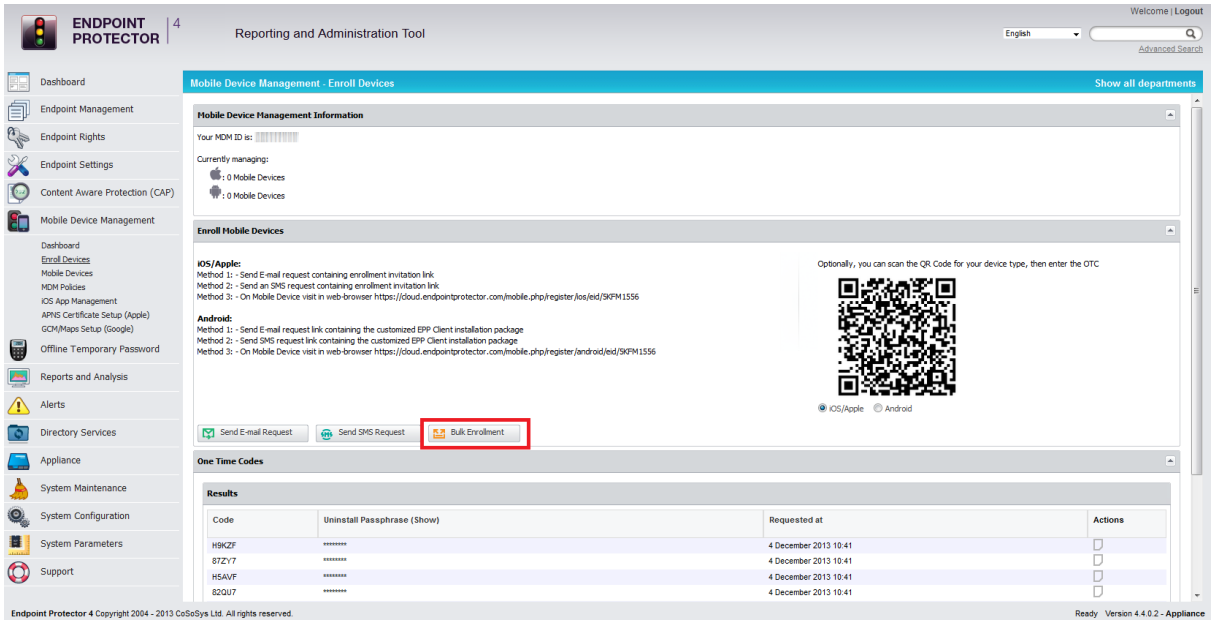
To enroll an Android mobile device, a Google Account is required to be previously setup by the user on the device. This is usually done when the user receives a new device and starts using it. Additionally, an Internet connection is mandatory for the communication between Endpoint Protector Appliance and the Android device. At least a 3G data connection is recommended to allow the communication with Google and Endpoint Protector Appliance and the transmission of the mobile device information.

Once the user has received the invitation and clicked on the included link, a confirmation page will be displayed in his browser, auto-filled with the MDM ID and OTC keys.

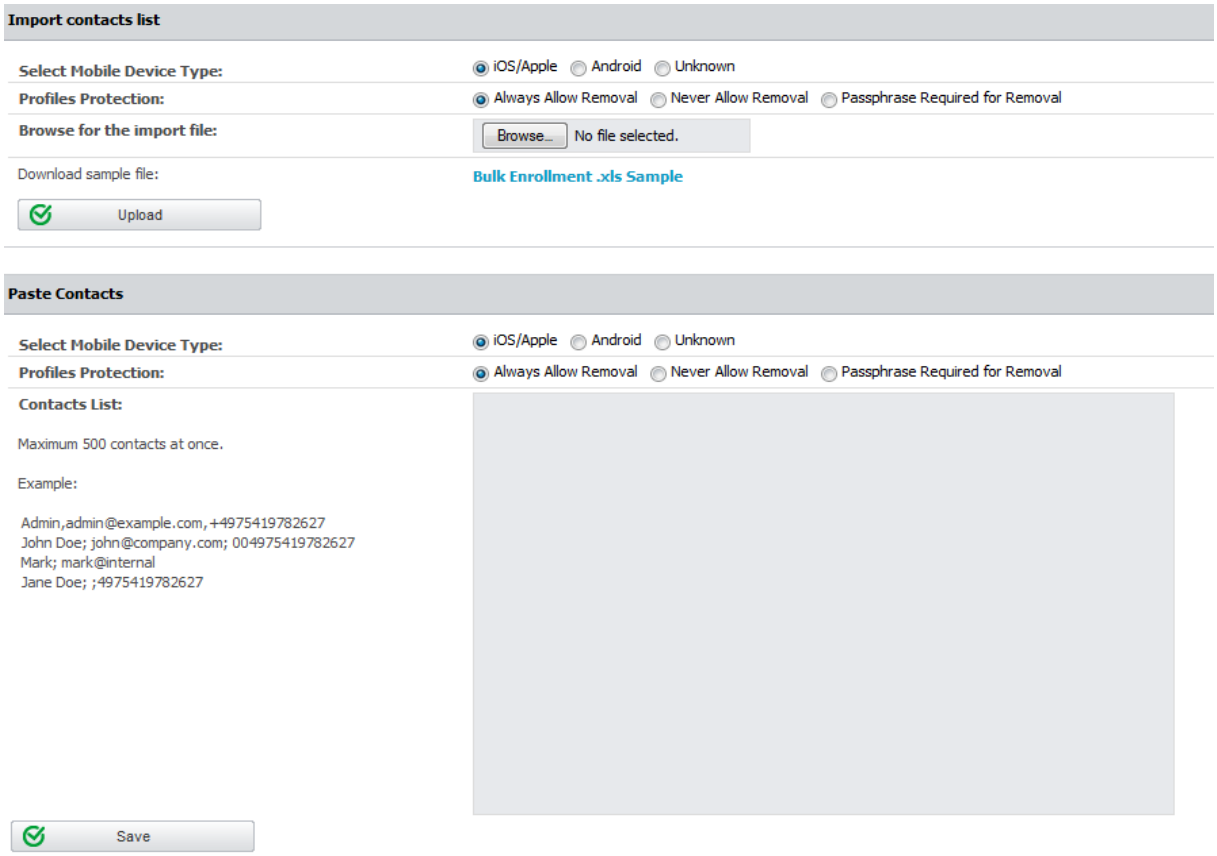
These steps are described in detail in chapter 6.4 Install EPP Client App on Android and Enrolling Android Device.

7.2.10. Bulk Enrollment

Bulk enrollment allows the administrator to send enrollment invitations to a large number of devices at the same time, through contacts list.



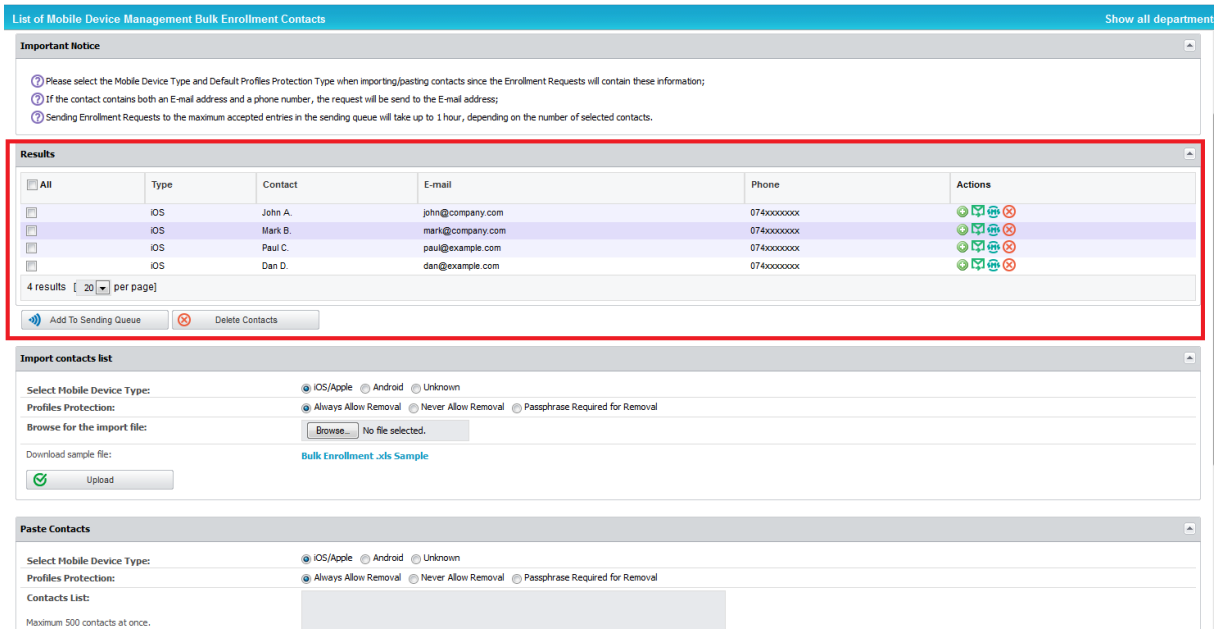
Contacts list can be imported from an .xls file or can be created in the „Paste Contacts" section.



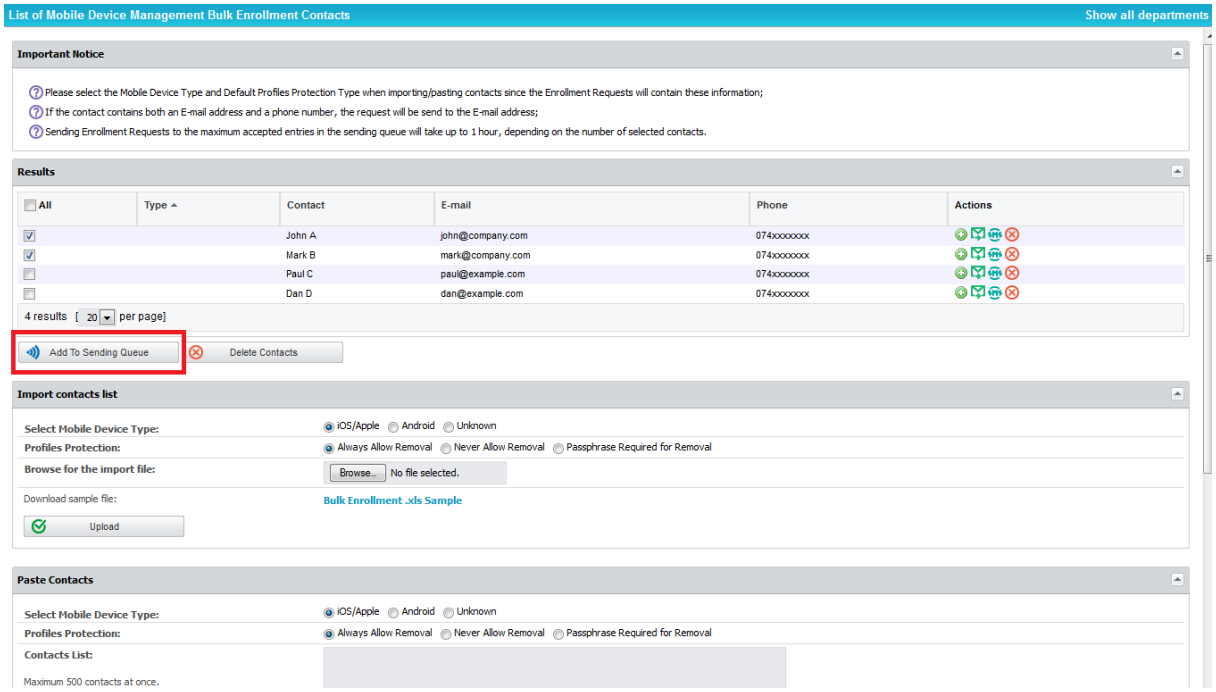
It is possible to paste up to 500 contacts at once. The required format is: name, separated with semicolon (;) the E-mail, separated with semicolon (;) the Telephone Number. (Example John A. ; john@company.com ; country_prefix-xxxxxx). Please note that a „Bulk Enrollment .xls Sample" file with a few examples inside is available for downloading.

Regardless of the way the contacts list is created, the mobile device type, and profile protection must be selected, otherwise a wrong enrollment link might be sent. Choose „Unknown" at „Select Mobile Device Type", if the devices to which the invitations will be sent are not just of one type(iOS, OS X or Android).

The added contacts will be available in the „Results" section.

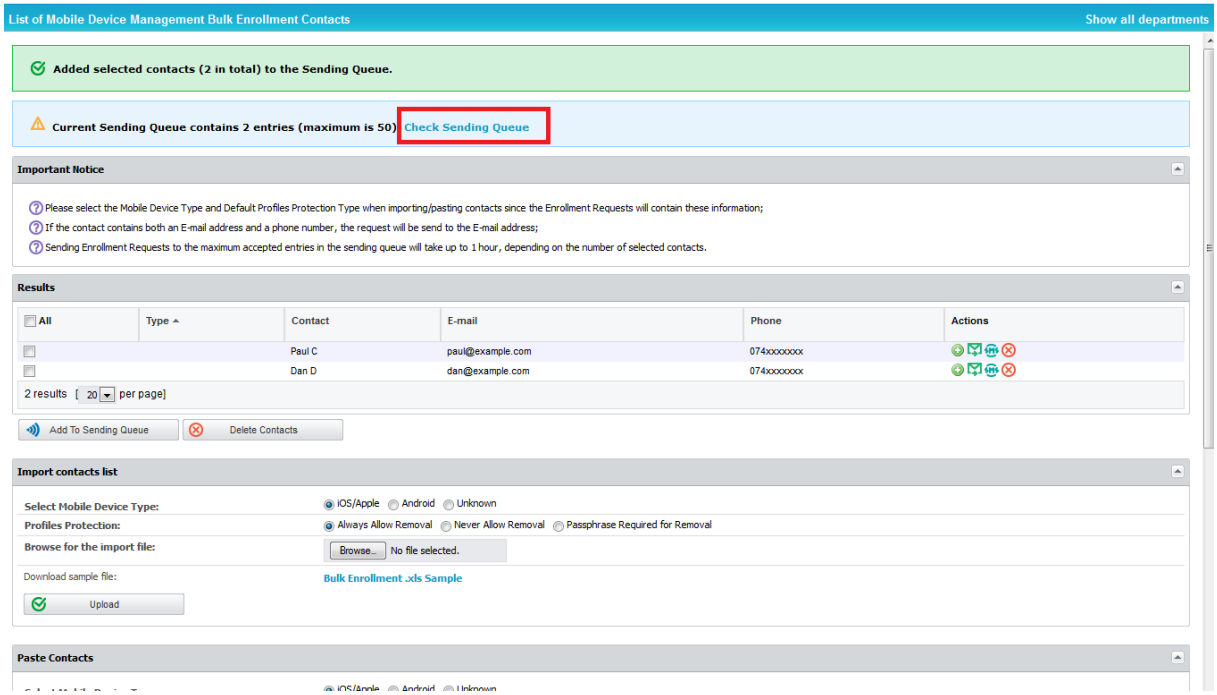


To add the selected contacts to the sending queue click on „Add To Sending Queue" button.



In case both e-mail and telephone number is given, the enrollment invitation will be sent via e-mail. Sending all the invitations might take up to one hour, depending on the number of selected contacts.

To view the pending enrollments click on the „Check Sending Queue" link.

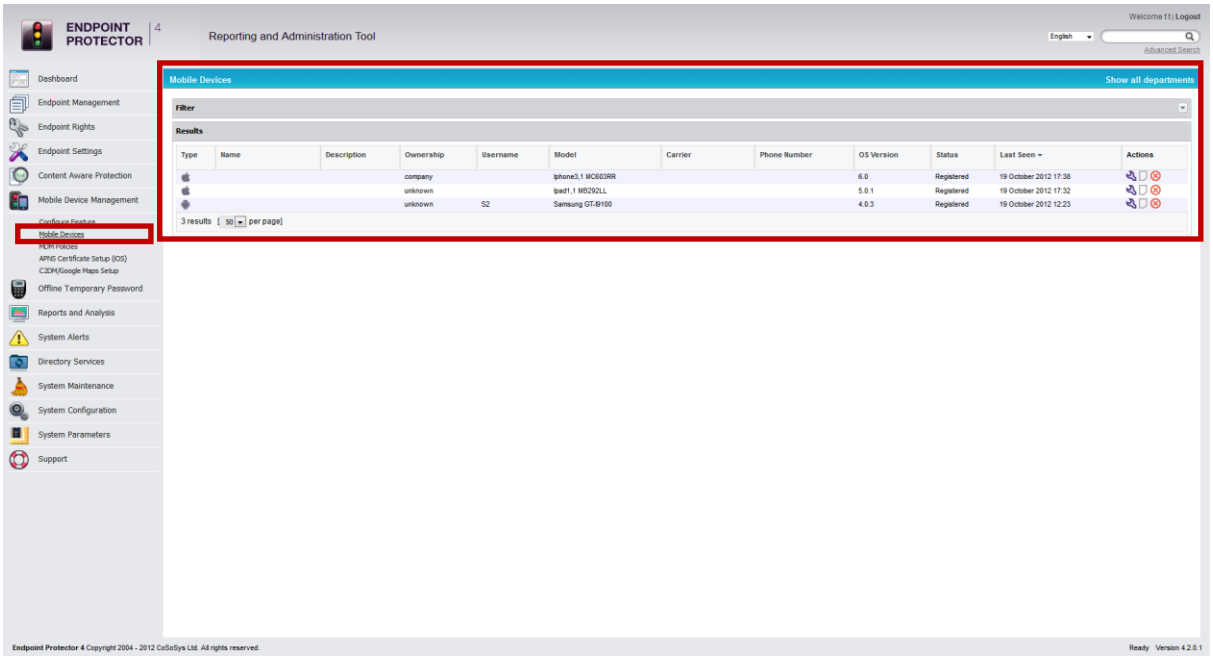

List of Mobile Device Management Bulk Enrollment Contacts
Show all departments
Added selected contacts (2 in total) to the Sending Queue.
Current Sending Queue contains 2 entries (maximum is 50)
Check Sending Queue
Important Notice
Please select the Mobile Device Type and Default Profiles Protection Type when importing/pasting contacts since the Enrollment Requests will contain these information;
If the contact contains both an E-mail address and a phone number, the request will be send to the E-mail address;
Sending Enrollment Requests to the maximum accepted entries in the sending queue will take up to 1 hour, depending on the number of selected contacts.
Results
All
Type
Contact
E-mail
Phone
Actions
Paul C
paul@example.com
074xxxxxxx
Dan D
dan@example.com
074xxxxxxx
2 results [20 per page]
Add To Sending Queue
Delete Contacts
Import contacts list
Select Mobile Device Type:
iOS/Apple
Android
Unknown
Profiles Protection:
Always Allow Removal
Never Allow Removal
Passphrase Required for Removal
Browse for the import file:
Browse...
No file selected.
Download sample file:
Bulk Enrollment .xls Sample
Upload
Paste Contacts

Note!

Contacts to which the invitations were already sent will no longer be available in the interface.

8. Managing Mobile Devices

The list of enrolled mobile devices and their status is available under Mobile Device Management -> Mobile Devices.



To manage a specific device, select it from the list by right-clicking on the device name and choose one of the available actions: **Manage Device (edit)**, **Hide, Show** and **Delete.**

Manage Device, *Hide,* *Delete*

The **Manage Device** option allows the Administrator to separately manage an already enrolled device and enforce different settings to the device such as security settings specifically for the selected device.

The **Hide** option once selected will remove the mobile device from the list without deleting the mobile device history or uninstalling / unmanaging the device. A hidden device can be added again to the list of mobile devices by selecting the "Show Hidden Devices" > Yes > "Apply Filter" option from the available Filter option.

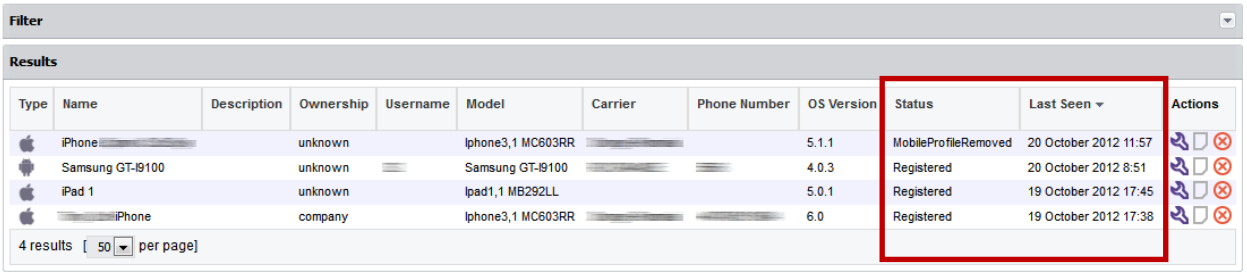
The **Delete** option once selected by the Administrator will delete a device and the corresponding history and logs from Endpoint Protector Appliance. We recommend not to "Delete" a device not before it was unmanaged. To unmanage a device, please check the section 15. Unmanage a Mobile Device in this manual.

Note!

We recommend using the "Hide" option instead of deleting the mobile device in order to keep the mobile device history for later auditing.

8.1. Mobile Device Status

Mobile Devices >



In the column Status the current mobile device status is shown if know to Endpoint Protector.

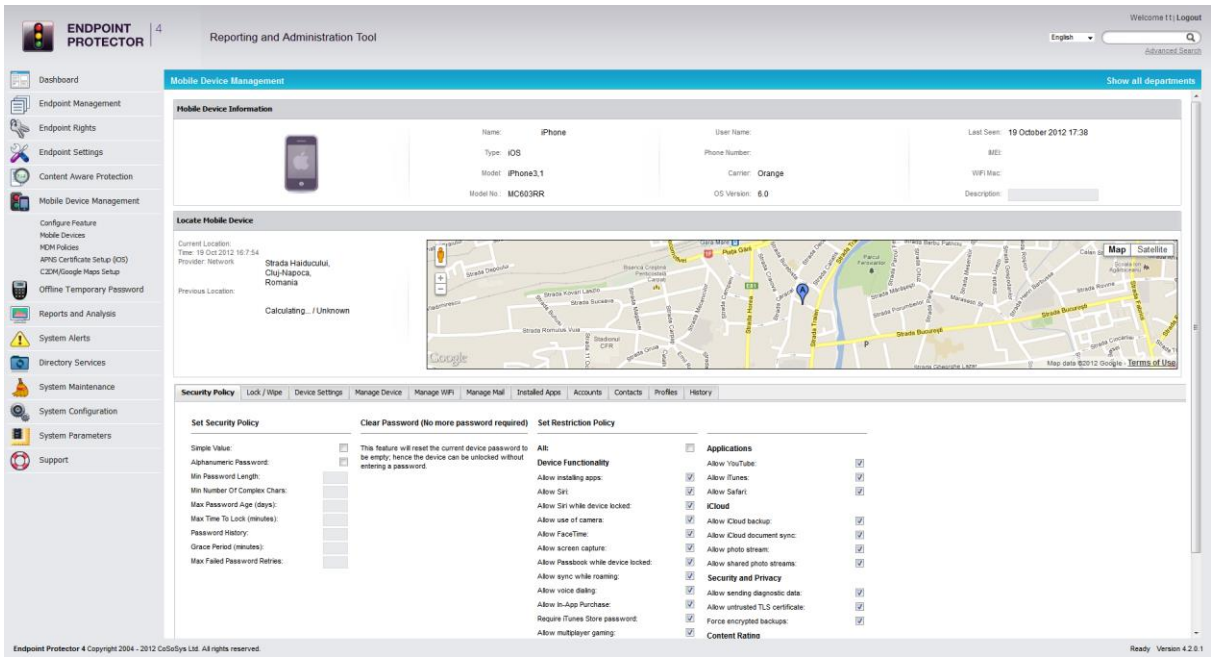
Registered – means the device is currently managed and Endpoint Protector MDM can communicate with the device. Applies to both iOS and Android devices.

MobileProfileRemoved – means the device is no longer managed. Either the device user has directly on the device removed the Enrollment Profile, or the Endpoint Protector Administrator has remotely removed the Enrollment Profile from the device to unmanage it. Applies to iOS devices.

DeviceAdminDisabled– means the device is no longer managed. Either the device user has directly on the device removed the EPP Client app, or the Endpoint Protector Administrator has remotely removed the EPP Client app from the device to unmanage it.

"Last Seen" is the time and date when the device has last time communicated with the Endpoint Protector MDM.

Selecting the "Manage Device" option for a mobile device will open the Manage Device page, containing different options to manage the selected device and to view information about it.



The main three rows are the following three:

- **Device Information**: displays all important device related details from mobile device name, model, type and OS to carrier related details such as carrier name, user phone number and user name. Not all information will be available all the time since the information available depends on the device and the operating system.

- **Locate Device**: displays on the included map the previous and the current location of the device at the time of the last request. By selecting the "Update Location" option, the current location will be displayed on the map, while the "Location History" option will allow the Administrator to view the previous locations of the mobile device. For iOS only the current location is available of the device. For Android all location options are available, while for OS X there is no location information available. Please remember, iOS and Android both require for location information the EPP MDM app to be installed on the device.

- **Device Management Tabs**: includes separate tabs containing the available MDM options for remote device and data managing. Detailed Features are described in the following paragraphs.

For each of the available Mobile Device Management options a status bullet is displayed indicating the returned result of a selected/executed operation:

Red indicates that the requested operation has failed.

Green indicates that the requested operation was successfully performed.

Yellow indicates that the requested operation is in pending mode.

A practical example is when you click on "Refresh Device Details". The bullet will turn yellow and stay for a few seconds in the yellow color until the request has been sent to the device and the device has answered to the Endpoint Protector Appliance. Then the status is changed to green and in this case the updated device details can be viewed.

Note!

Due to the differences existing between the iOS, OS X and Android platforms, some of the MDM features might not be available for all OS.

8.1.1. Available Options

The table below shows the available MDM options for Android and iOS mobile Devices. More options will be made available updated with each version update.

Tab	MDM Option	Description	OS Support
Device Settings	Device Ownership	Allows to define the owner of the device: Personal, Company or Unknown	/ / OSX
Device Settings	Voice Roaming	Allows to deactivate the Voice Roaming service for the mobile device (*Carrier dependent)	
Device Settings	Data Roaming	Allows to deactivate the Data Roaming service for the mobile device	
Device Settings	Device Location Settings	Allows to set additional parameters for the locating option: Location Accuracy Fine & Location Cost Allowed for a more accurate mobile device locating	/
Lock / Wipe	Lock Device	Remotely locks the user mobile device with or without resetting the user's password	/ / OSX
Lock / Wipe	Wipe Device Data	Remotely deletes all device data. Additionally, the data stored on the SD Card can be deleted as well by checking the "Include SD Card" option	/ / OSX
Lock / Wipe	Wipe SD Card	Remotely deletes all data stored on the SD Card	
Security Policy	Current Security Policy	Displays the security settings applied at that moment	/ / OSX
Security Policy	FileVault 2 Disk Encryption	Encrypts the content of the disk automatically	OSX
Security Policy	Set Security Policy	Allows defining additional password settings such as: minimum password length, password quality, max. time to lock, max. number of password retries before wipe.	/ / OSX
Security Policy	Ask User To Change Password	Enforces the user to define a new password	/ / OSX
Security Policy	Clear Password	Resets any existing password for the mobile device	
Security Policy	Device Password	Resets any existing password and allows defining remotely a different password for the mobile device	/ / OSX

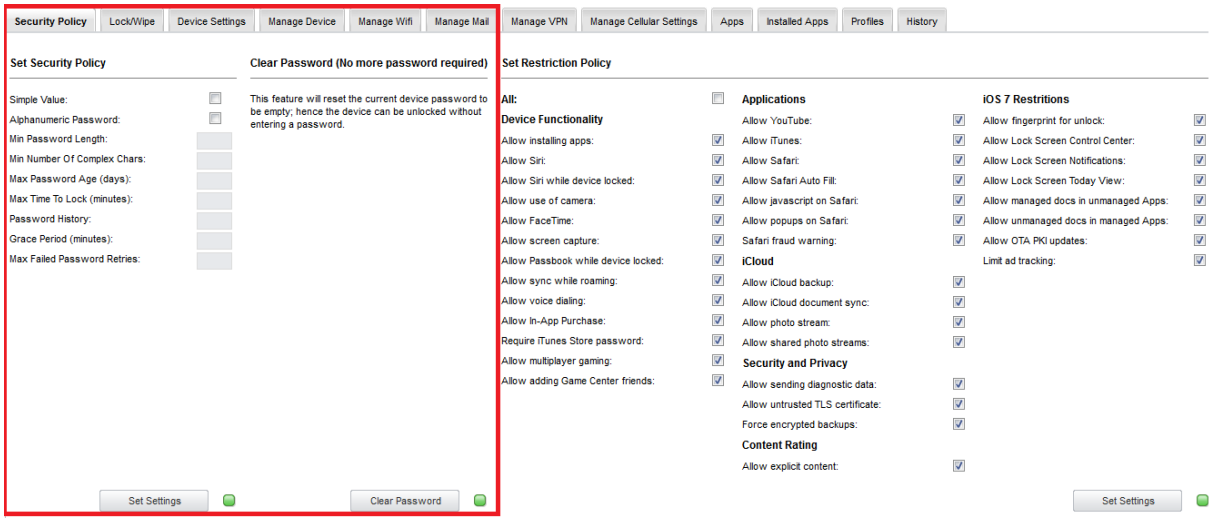
Security Policy	Password History	Keeps a track of the last passwords used and doesn't allow setting them as new passwords	
Security Policy	Password Age	Enforces the user to define a new password after a certain time period	/ OSX
Security Policy	Grace Period	Enforces the user to define a new password after the grace period is over (counted in minutes)	/ OSX
Manage Device	Play Sound on Device	Activates a song on the device, which will play for a predefined period of time	
Manage Device	Refresh Device Details	Updates the device details displayed under Device Information	/ / OSX
Manage Device	Refresh App List	Display the list of currently installed apps on the mobile device	/ / OSX
Manage Device	Refresh Profile List	Display the list of currently set profiles on the mobile device	/ OSX
Manage Device	Refresh Google Accounts	Display the list of currently set Google e-mail accounts on the mobile device	
Manage Device	Refresh Accounts	Display the list of all currently set e-mail accounts on the mobile device	
Manage Device	Refresh Contacts	Display the list of all current contacts saved on the mobile device	
Installed Apps	Installed Apps	Shows the list of installed apps after selecting the Refresh Apps List option	/ / OSX
Remove Installed Apps	Installed Apps	Removes the selected application from the list of installed apps and uninstalls the application from the mobile device	
Accounts	Accounts	Shows the list of e-mail accounts after selecting the Refresh Accounts / Refresh Google Accounts option	
Contacts	Contacts	Shows the list of contacts after selecting the Refresh Contacts option	
Profiles	Profiles	Shows the list of set profiles after selecting the Refresh Profile List option	/ OSX
History	History	Logs all device activity	/ / OSX

9. Manage iOS Devices

For each operating system (iOS, OS X and Android) different Device Management features are supported and available. For iOS the different management settings are stored as different profiles. One iOS device can have multiple profiles stored on it.

9.1. Security Settings (Security Profile) on iOS

Enforcing the use of a password / passcode is the most important feature on any device, company or individually owned. Protecting access to data on the device is the first task to protecting your iOS devices.



9.1.1. Password / Passcode Setting on iOS Device

Mobile Devices > Security Policy > Set Security Policy

The following Settings can be applied for the password / passcode settings for an iOS device:

- **Simple Value** – Example Password could be 1221
- **Alphanumeric Password** – Example could be 123A
- **Min Password Length** – Minimum number of digits
- **Min Number Of Complex Chars** – Minimum number of complex characters. Complex characters are for example: !@#$%&* etc.
- **Max Password Age (days)** – Number of days for which a user can use the same password. After that the user is requested to change the password to a new password.
- **Max Time To Lock (minutes)** – If iOS device is not used the device will lock (request password to access again) after set number of minutes.
- **Password History** – When a new password is set a new password is required. For example, if set to two, it means that after changing the password the user cannot reuse a previously used password until he has set two new passwords in the meantime.
- **Grace Period (minutes)** – Means the time a user has to make a change to the password or to initially set a password after the device receives the security policy.
- **Max Failed Password Retries** – Means the number a user can enter a wrong password until the device will wipe all data and reset itself. In case of reset, the device is wiping its entire data and is reset to a factory default. All data on the device is erased and cannot be recovered.

9.1.2. Clear Passcode (No more password required)

Using the option "Clear Passcode" the current device password will be set to be empty; hence the device can be unlocked without entering a password. This feature can be helpful in case the device is damaged and a password cannot be entered through the device itself.

9.1.3. iOS Device Hardware Encryption

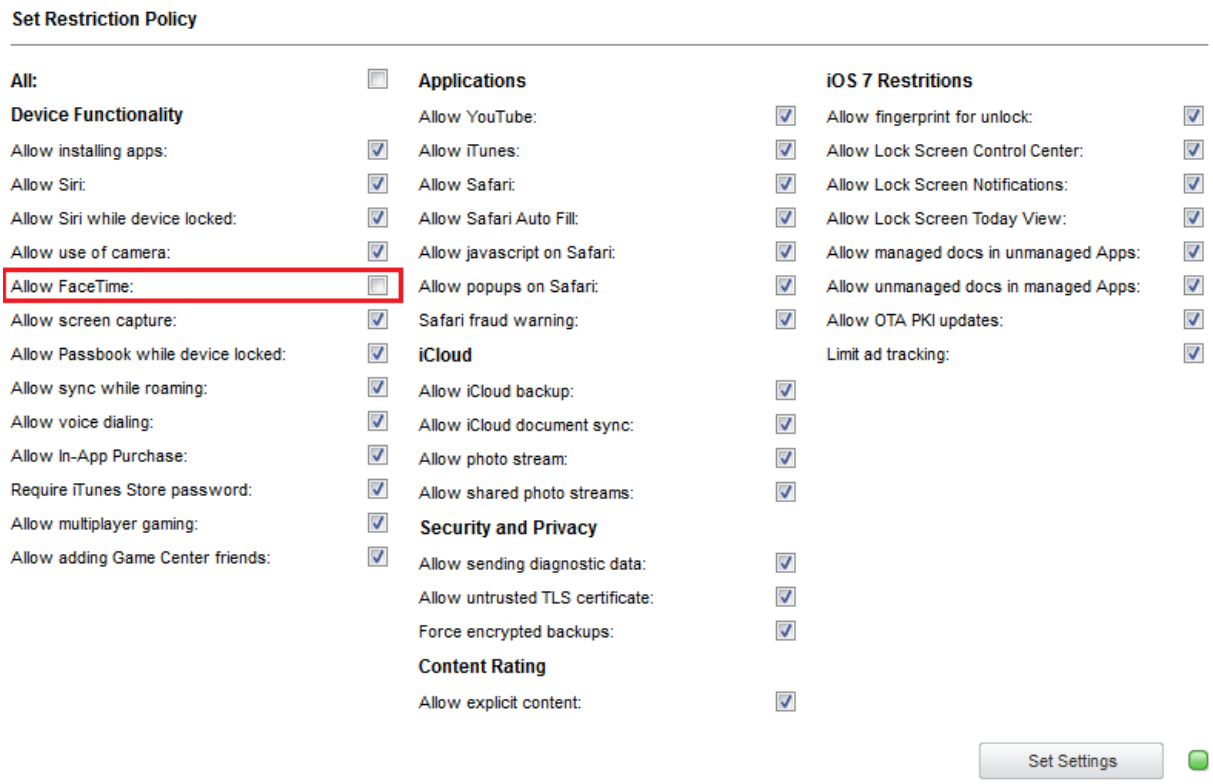
When the password/code for an iOS device is set the iOS device is automatically using its built in hardware encryption in order to protect data on the device in case it is lost or stolen. We recommend setting a complex password in the security policy in order to have maximum protection.

9.2. Restrictions (Restrictions Profile) on iOS

Mobile Devices > Security Policy > Set Restriction Policy

In order to use an iOS according to a company policy the Endpoint Protector Administrator can choose what options / features to allow to be used on the iOS device or to be disabled.

Disabling an option / feature will result in the option / feature being disabled from the iOS device. A practical example would be for the Administrator to disable the use of FaceTime. After the restriction policy is received by the iOS device, the FaceTime app icon and all FaceTime related options under Settings are removed (see screenshots below). The iOS device user has no option anymore to access or use the FaceTime feature.



Left image, FaceTime disabled (missing) by policy. Right image, FaceTime enabled without policy.

9.2.1. The following iOS features can be restricted

- Allow installing apps
- Allow Siri
    - Allow Siri while device locked
- Allow use of camera
- Allow FaceTime
- Allow screen capture
  (making screenshots feature, holding home button and ON/OFF button to capture screen)
- Allow Passbook while device locked
- Allow sync while roaming
- Allow voice dialing
- Allow In-App Purchase
- Require iTunes Store password
- Allow multiplayer gaming
- Allow adding Game Center friends

9.2.2. The following Applications can be restricted

- Restrict YouTube App (native iOS YouTube)
  Since YouTube is not part of iOS 6 anymore this feature is only supported for iOS 4 and iOS 5.
- Allow iTunes
- Allow Safari
- Allow Safari Auto Fill
- Allow javascript on Safari
- Allow popups on Safari
- Safari fraud warning

9.2.3. iCloud restrictions / Photo stream restrictions

iCloud is a service where almost all data on an iOS device is uploaded to Apple Servers. Some companies might choose to restrict the use of iCloud due to regulatory requirements, compliance requirements, data protection concerns or simply privacy concerns.

- Allow iCloud backup
- Allow iCloud document sync
- Allow photo stream
- Allow shared photo streams
  Disallow photo stream can cause loss of data that was part of photo stream.

9.2.4. Security and Privacy Restrictions

- Allow sending diagnostic data
- Allow untrusted TLS certificate
- Force encrypted backups (when backing up iOS device to a computer)

9.2.5. Content Rating Restrictions

- Allow explicit content

9.2.6. iOS7 Restrictions

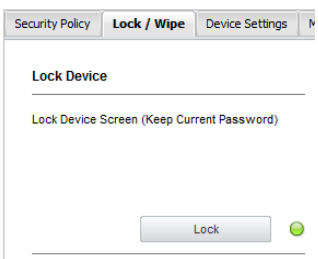
- Allow fingerprint for unlock
- Allow Lock Screen Control Center
- Allow Lock Screen Notifications
- Allow Lock Screen Today View
- Allow managed docs in unmanaged Apps
- Allow unmanaged docs in managed Apps
- Allow OTA PKI updates
- Limit ad tracking

9.2.7. Supervised Device Restrictions

- Allow AirDrop
- Allow Account Modification
- Allow App Cellular Data Changes
- Allow User Generated Siri Content
- Allow changes to Find My Friends
- Allow Host Pairing
- Allow iBookstore
- Allow Game center
- Allow iMessage
- Allow App Removal

9.3. Remote iOS Lock of Device

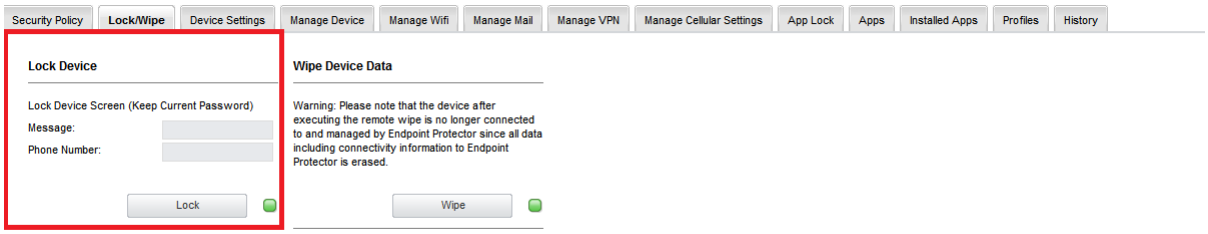
Mobile Devices > Lock / Wipe > Lock Device



The iOS device can be remotely locked. Clicking "Lock" will remotely lock the device screen and require a password entry to unlock the screen. The current password is kept in this case if the device is remotely locked.

The remote lock of a device works also in case of a device that has a SIM card and the SIM card has been removed from the device. As long as the device has a working internet connection, in this case over Wi-Fi the remote locking of the device will still work as long as the lock command can reach the device.

On Supervised iOS 7 devices it is possible to show a message and a phone number when locking the screen. For the message and phone number to appear the device must have a previously set password.



9.4. Remote iOS Device Wipe (Device Nuke)

Mobile Devices > Lock / Wipe > Wipe Device Data

Security Policy
Lock / Wipe
Device Settings
Manage Device
Manage WiFi
Manage Mail
Installed Apps
Lock Device
Lock Device Screen (Keep Current Password)
Lock
Wipe Device Data
Warning: Please note that the device after executing the remote wipe is no longer connected to and managed by Endpoint Protector since all data including connectivity information to Endpoint Protector is erased.
Wipe

The iOS device can be remotely wiped. A remote wipe will erase all data on the device and reset the device to its factory default. To remotely wipe a device click "Wipe" and a confirmation message will ask to proceed if you are sure you want to remotely wipe the device.

After a remote wipe the device is unmanaged. No more connection between the iOS device and Endpoint Protector is possible after the remote wipe.

The remote wipe of a device works also in case of a device that has a SIM card and the SIM card has been removed from the device. As long as the device has a working internet connection, in this case over Wi-Fi the remote wipe of the device will still work as long as the wipe command can reach the device.

Note!

All data on the device will be permanently lost. It cannot be recovered after a remote wipe. Use this feature with caution and only as a last resort.

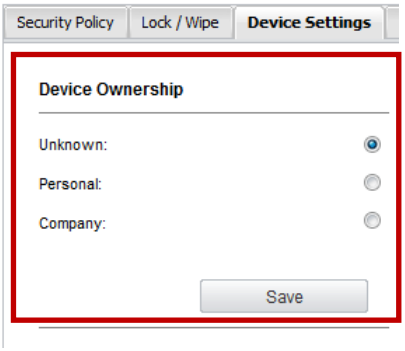
9.5. iOS Disable Device Password / Passcode

Mobile Devices > Security Policy > Clear Password (No more password required)

The option "Clear Password (No more password required)" will disable the password / passcode requirement for the iOS device. Unlocking the device screen will be possible without a password entry.

9.6. Device Ownership

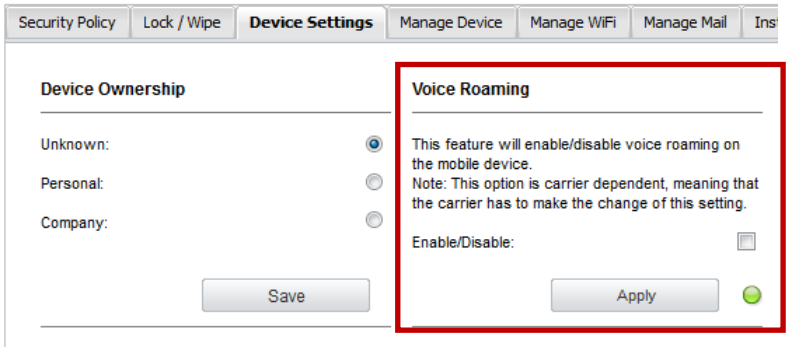
Mobile Devices >Device Settings > Device Ownership



The option "Device Ownership" can be set to who is the rightful owner of a device. Set it to "Company" if the company has purchased the device for the user or to "Personal" if the user has purchased the device and uses it for business purposes. After a device is enrolled the default settings is set to "Unknown".

9.7. Voice Roaming on iOS

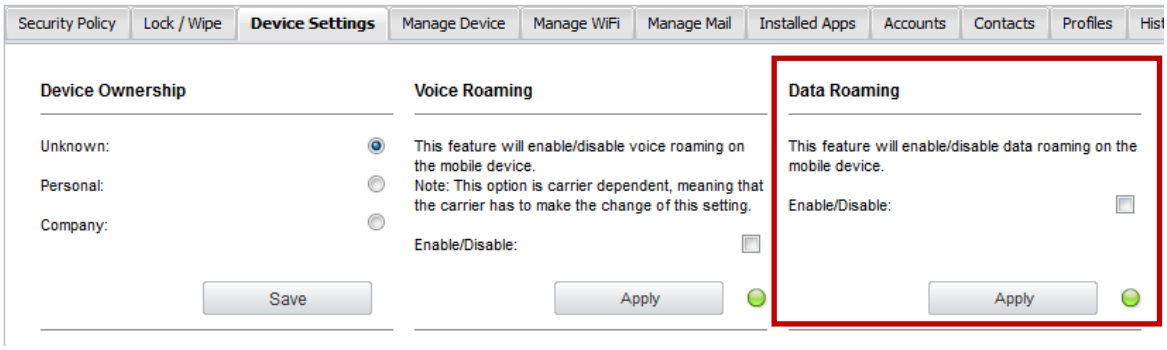
Mobile Devices >Device Settings > Voice Roaming



The option "Voice Roaming" can be set to allow a device to have voice roaming enabled while outside of range of the default cellular network. This setting can in some cases also bed dependent on the cellular network provider. It might be required depending on the cellular subscription if voice roaming has to be activated first for the subscription before it can be enabled or disabled through Endpoint Protector.

9.8. Data Roaming on iOS

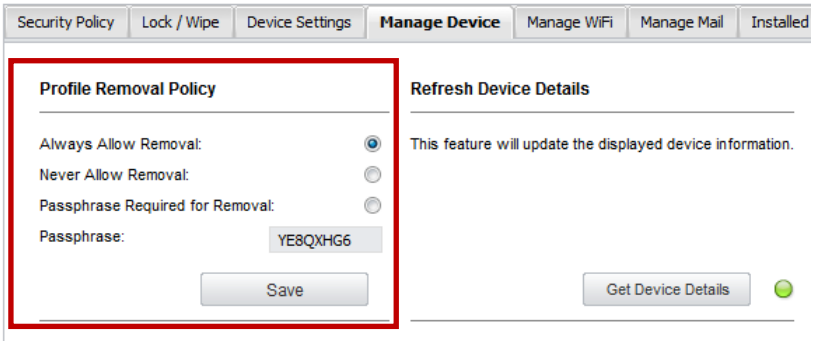
Mobile Devices >Device Settings > Data Roaming



The option "Data Roaming" can be set to allow a device to have data roaming enabled while outside of range of the default cellular network. This setting can in some cases also be dependent on the cellular network provider. It might be required depending on the cellular subscription if data roaming has to be activated first for the subscription before it can be enabled or disabled through Endpoint Protector MDM.

9.9. Profile Removal Policy for iOS Devices

Mobile Devices > Manage Device > Profile Removal Policy

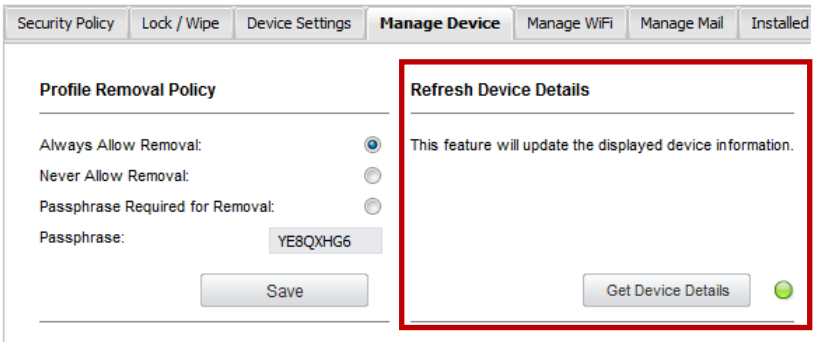


As described in the chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase before the profiles (settings) on an iOS Device can be protected with a passphrase. In this option the passphrase can be changed to be a different one than the one automatically generated and associated with the OTC. For the full

description of this option please consult chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase.

9.10. Refresh Device Details for iOS

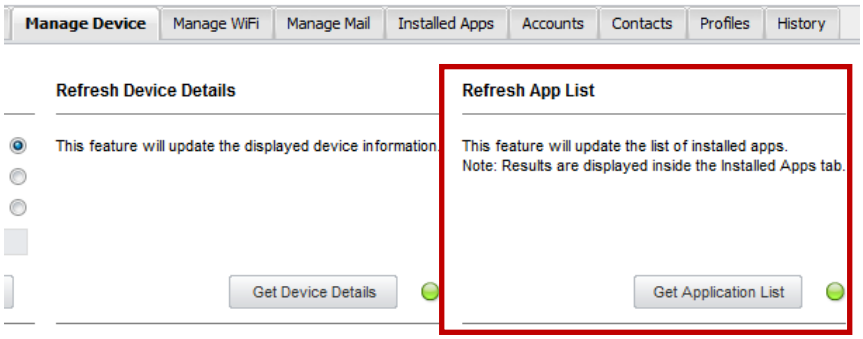
Mobile Devices > Manage Device > Refresh Device Details



This function will ask the iOS devices for its latest details and display them in the Mobile Device Information section.

9.11. Refresh App List for iOS

Mobile Devices > Manage Device > Refresh App List

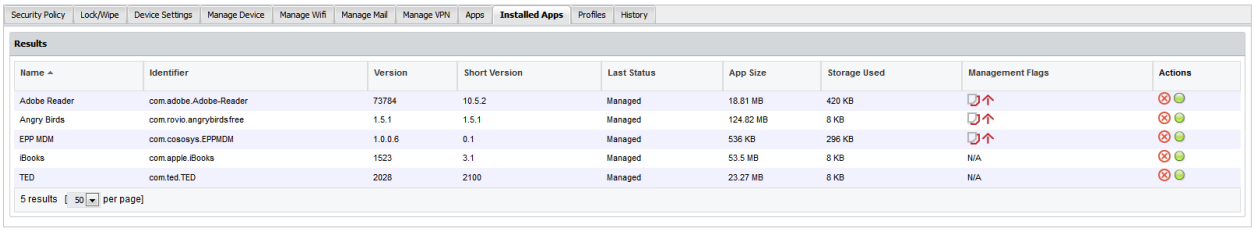


This function by clicking "Get Application List" will ask the iOS device for a list of all the apps installed on the iOS device. The list of all installed Apps is shown in Endpoint Protector MDM at Mobile Devices > Installed Apps. If the user installs a new application, the list of the installed apps will be updated next time when the administrator will request the list of apps by pressing the "Get Application List" button.

9.12. Installed Apps on iOS

Mobile Devices > Installed Apps

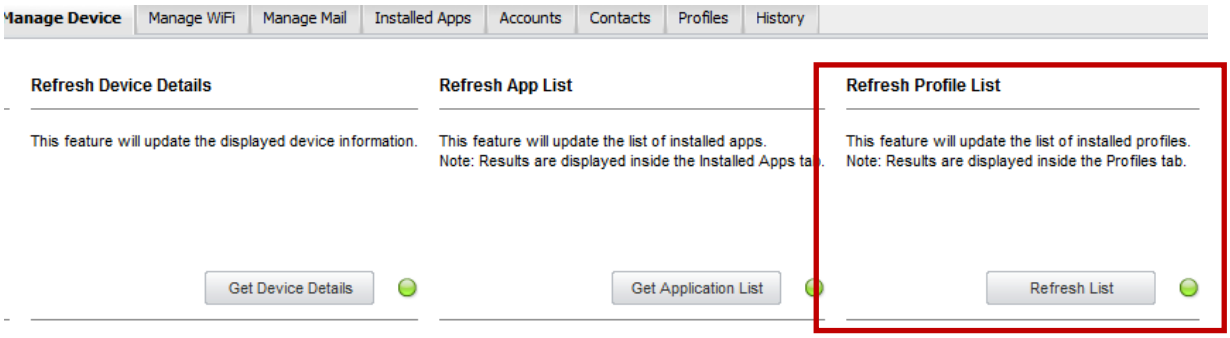
The List of Apps installed on the iOS device lets the Administrator see what apps users have installed on their devices. The list of apps installed on a device can be requested from the iOS device and updated though the option "Get Application List" as described in chapter 9.11 Refresh App List for iOS.



Installed Apps on managed iOS devices can be pushed, uninstalled and managed in different ways as described in the chapter 12 Mobile Application Management (MAM) for iOS.

9.13. Refresh Profile List on iOS

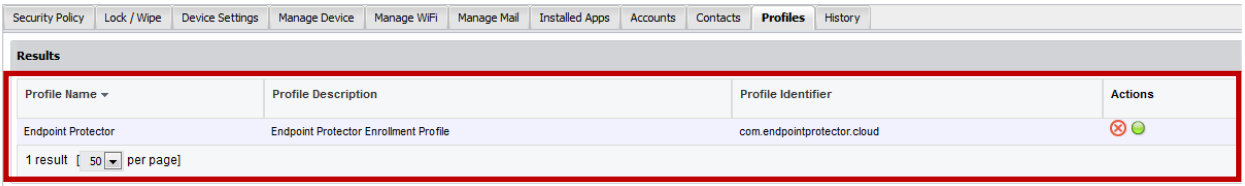
Mobile Devices > Manage Device > Refresh Profile List



The Profile List of an iOS device will show you what profiles are currently installed on the device. The list of installed profiles is shown here Mobile Devices > Profiles.

9.14. Profiles on iOS Devices Information

Mobile Devices > Profiles



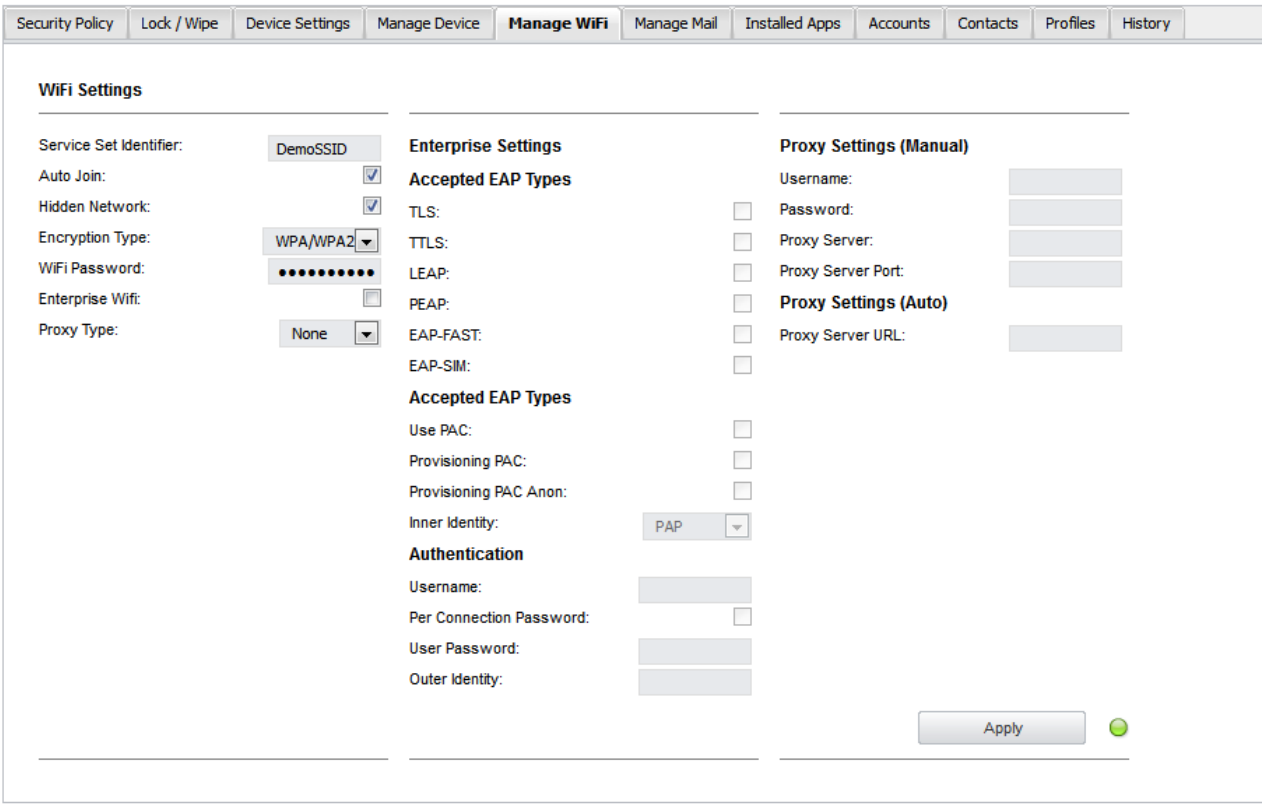
The profiles installed on an iOS Device are listed in the "Profile" tab. The Profiles installed on an iOS Device are always the enrollment Profile and possible restriction or other profiles. The type of profile is shown in the "Profile Description" column.

9.14.1. Remove Profile from iOS Device

From here the Endpoint Protector Administrator can also perform the remove action of a profile by clicking on "Remove Profile". If a profile, e.g. a Restriction Profile is removed, the associated restrictions from the iOS device are removed. In case the Administrator want to unmanage a device, the Enrollment Profile needs to be removed. After removing the enrollment profile the device is no loger managed.

9.15. Manage WiFi on iOS

Mobile Devices > Manage WiFi



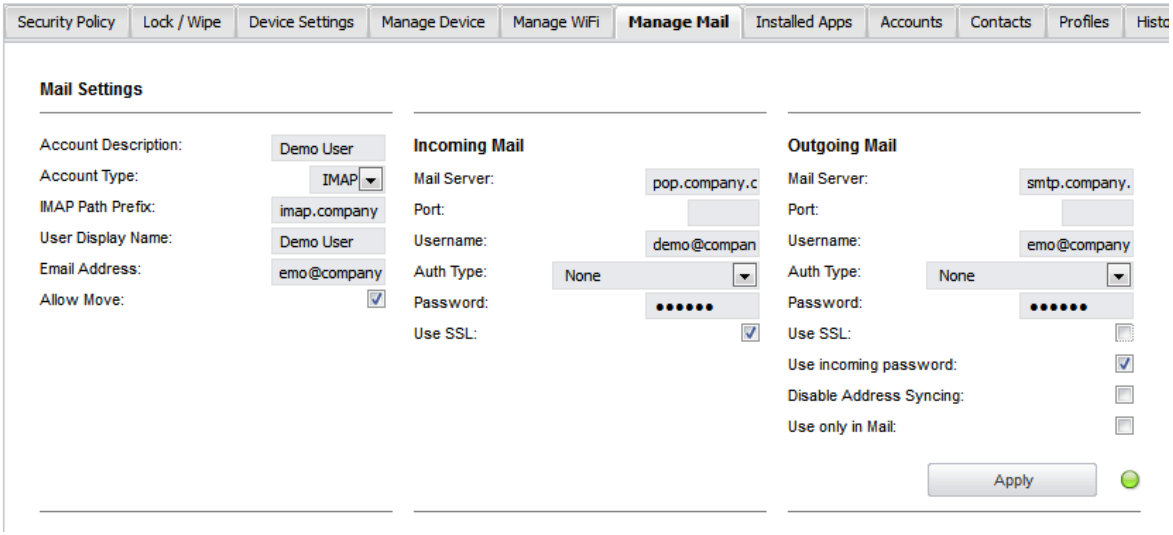
The Endpoint Protector Administrator can apply wireless network (WiFi) settings to an iOS device. This can be used for iOS devices to automatically connect to a WiFi access point without having to manually add the settings on the device.

9.15.1. Wipe Wi-fi Settings

Wi-Fi Profile can be removed to wipe company Wi-Fi Settings while personal Wi-Fi content remains untouched.

9.16. Manage Mail on iOS

Mobile Devices > Manage Mail



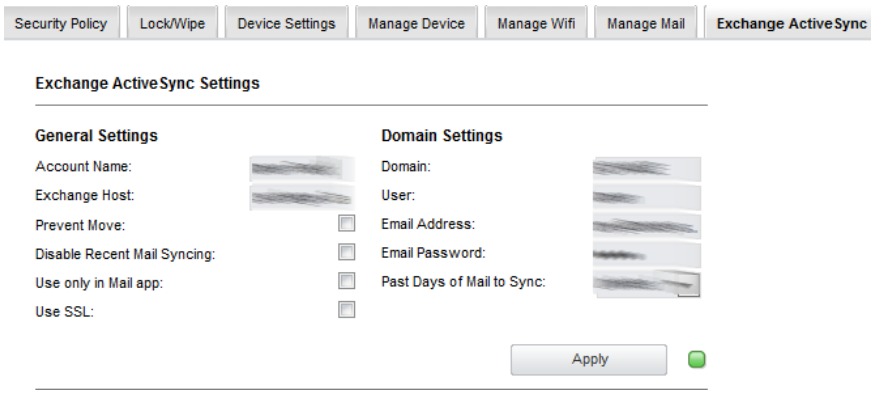
The Endpoint Protector Administrator can apply E-Mail settings to an iOS device. This can be used for iOS devices to automatically use company e-mail accounts and settings without having to manually add the settings on the device.

9.16.1. Wipe E-mail Settings

E-mail Profile can be removed to wipe company E-Mail Content and Settings while personal E-mail accounts and content remain untouched.

9.17. Exchange Active Sync

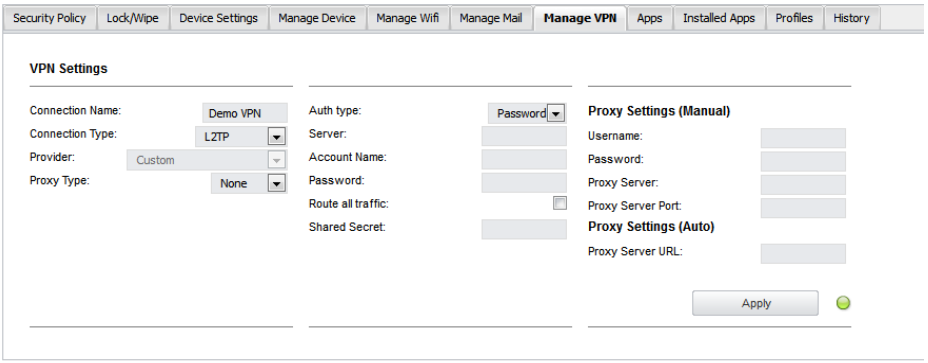
Mobile Devices > Exchange Active Sync



The Endpoint Protector Administrator can apply Exchange Account settings to an iOS device. This can be used for iOS devices to automatically use company e-mail accounts and settings without having to manually add the settings on the device.

9.18. Manage VPN on iOS

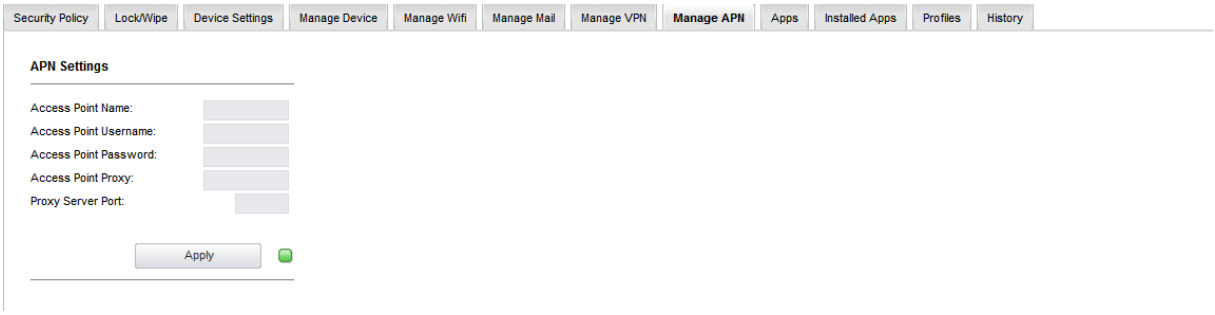
Mobile Devices > Manage VPN



The Endpoint Protector Administrator can apply VPN settings to an iOS device. This can be used for iOS devices to automatically deploy and use company VPN settings and policies without having to manually add the settings on the device.

9.19. Manage APN settings on iOS

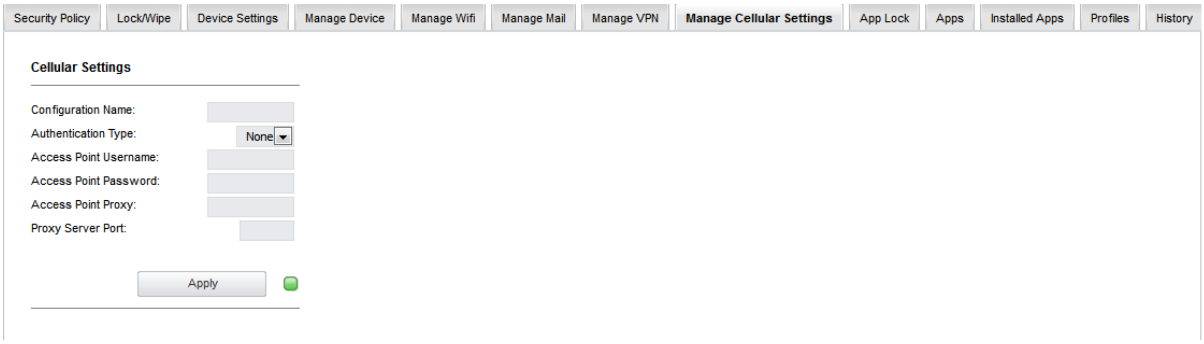
The Access Point Name (APN) defines the network path for all cellular data connectivity. You can view or edit the APN for cellular data services on iPhone or iPad, if your device uses a SIM card and you carrier allows you to edit the Access Point Name.



To change the settings on the target device, complete the required fields. You'll have to provide a name, access point username and password and proxy server if needed. Pressing "Apply" will push the cellular settings to the device.

9.20. Manage Cellular Settings on Supervised iOS 7 devices

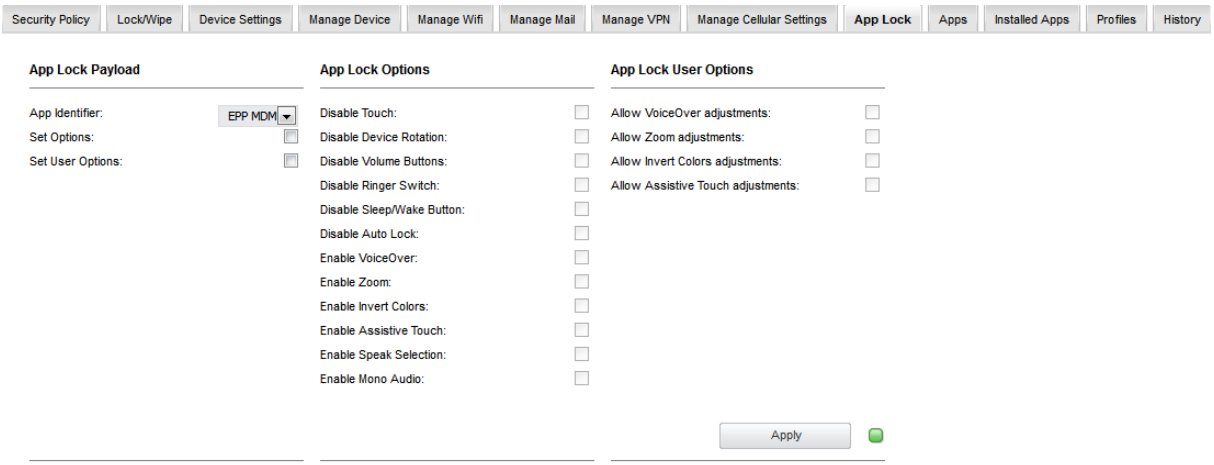
Cellular data is used for data communication in cellular networks. It doesn't affect your ability to make or receive phone calls or to use Wi-Fi networks for Internet connectivity.



To change the settings on the target device, complete the required fields. You'll have to provide a name, the authentication type, access point username and password and proxy server if needed. Pressing "Apply" will push the cellular settings to the device.

9.21. App Lock on Supervised iOS 7 devices

The App Lock feature can be used to lock a device so only one application, which will be set from the server, can run on it. This feature is only available on Supervised iOS 7 devices.



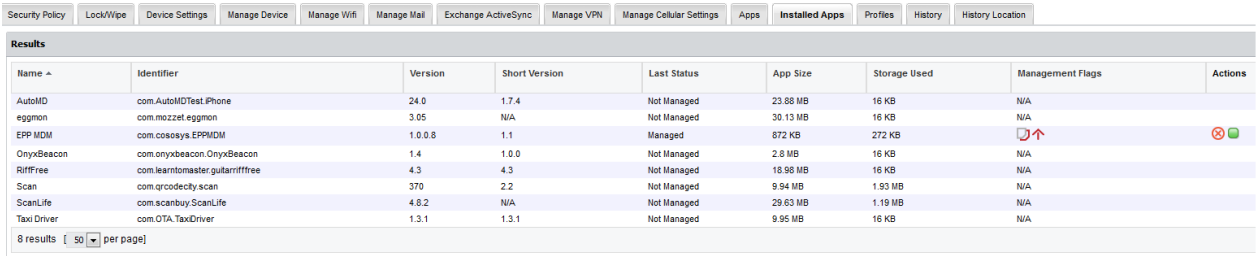
If the list of existing applications on the device was never updated on the server, it is a must to press the "Get App List" button from the Manage Device section as explained in paragraph 9.11, otherwise there will be no application listed in the "App Identifier" dropdown. However, it is recommended to use "Get App List" each time before the App Lock feature is used to refresh the available apps.

After interrogating the device for the available apps, it is possible to set some further options which will define the usability of the application. Finally pressing the "Apply" button will enforce the App Lock on the device.

9.22. Installed Apps

Mobile Devices > Installed Apps

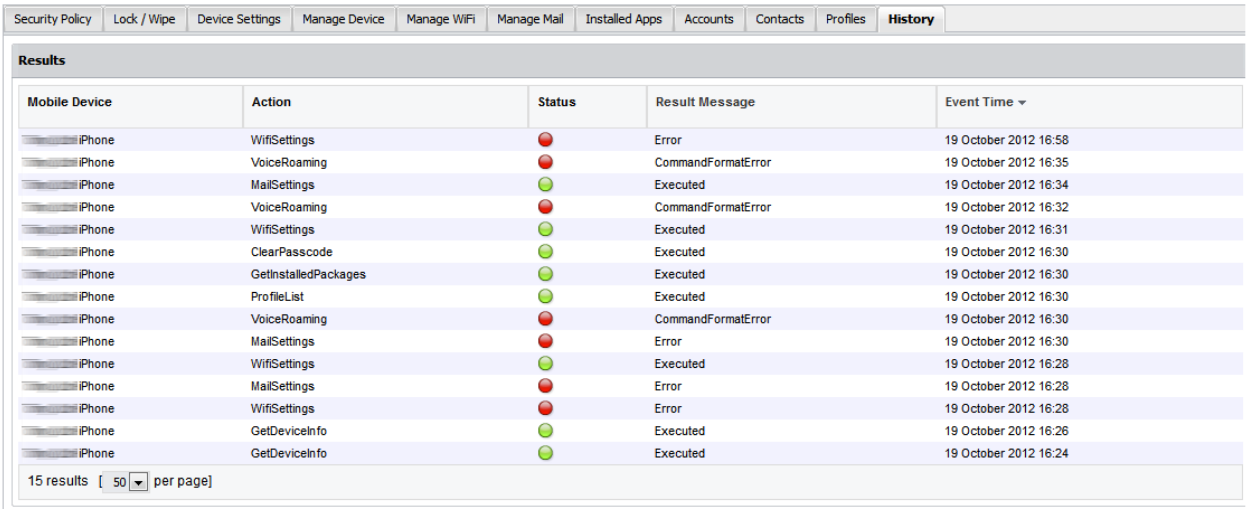
A list of applications already installed on an iOS device can be seen in the "Installed Apps" tab. The list includes apps pushed through Endpoint Protector as well as apps installed directly from the mobile device.


Security Policy
Lock/Wipe
Device Settings
Manage Device
Manage Wifi
Manage Mail
Exchange ActiveSync
Manage VPN
Manage Cellular Settings
Apps
Installed Apps
Profiles
History
History Location
Results
Name
Identifier
Version
Short Version
Last Status
App Size
Storage Used
Management Flags
Actions
AutoMD com.AutoMDTest.iPhone 24.0 1.7.4 Not Managed 23.88 MB 16 KB N/A
eggmon com.mozzet.eggmon 3.05 N/A Not Managed 30.13 MB 16 KB N/A
EPP MDM com.cososys.EPPMDM 1.0.0.8 1.1 Managed 872 KB 272 KB
OnyxBeacon com.onyxbeacon.OnyxBeacon 1.4 1.0.0 Not Managed 2.8 MB 16 KB N/A
RiffFree com.learntomaster.guitarrifffree 4.3 4.3 Not Managed 18.98 MB 16 KB N/A
Scan com.qrcodecity.scan 370 2.2 Not Managed 9.94 MB 1.93 MB N/A
ScanLife com.scanbuy.ScanLife 4.8.2 N/A Not Managed 29.63 MB 1.19 MB N/A
Taxi Driver com.OTA.TaxiDriver 1.3.1 1.3.1 Not Managed 9.95 MB 16 KB N/A
8 results [50 per page]

9.23. History of iOS Devices Actions

Mobile Devices > History

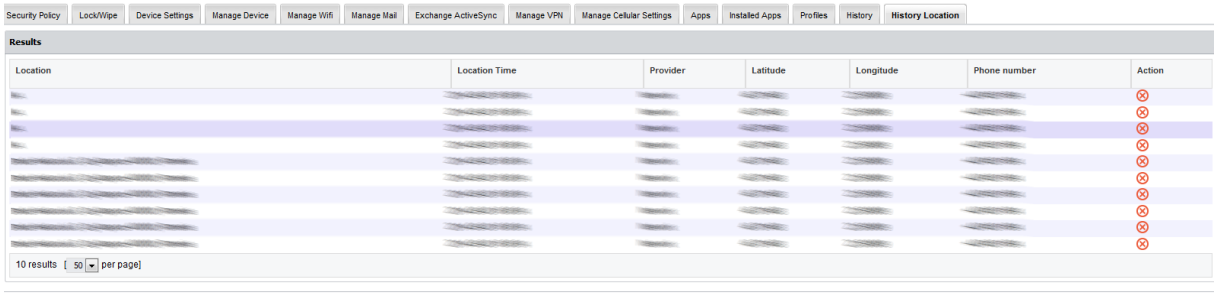
In the "History" tab, a record of actions sent to an iOS device are saved and the corresponding results are shown as well. The result can be executed, error, failed or pending.


Security Policy
Lock / Wipe
Device Settings
Manage Device
Manage WiFi
Manage Mail
Installed Apps
Accounts
Contacts
Profiles
History
Results
Mobile Device
Action
Status
Result Message
Event Time
iPhone WifiSettings Error 19 October 2012 16:58
iPhone VoiceRoaming CommandFormatError 19 October 2012 16:35
iPhone MailSettings Executed 19 October 2012 16:34
iPhone VoiceRoaming CommandFormatError 19 October 2012 16:32
iPhone WifiSettings Executed 19 October 2012 16:31
iPhone ClearPasscode Executed 19 October 2012 16:30
iPhone GetInstalledPackages Executed 19 October 2012 16:30
iPhone ProfileList Executed 19 October 2012 16:30
iPhone VoiceRoaming CommandFormatError 19 October 2012 16:30
iPhone MailSettings Error 19 October 2012 16:30
iPhone WifiSettings Executed 19 October 2012 16:28
iPhone MailSettings Error 19 October 2012 16:28
iPhone WifiSettings Error 19 October 2012 16:28
iPhone GetDeviceInfo Executed 19 October 2012 16:26
iPhone GetDeviceInfo Executed 19 October 2012 16:24
15 results [50 per page]

9.24. History Location

Mobile Devices > History Location

The “History Location” tab shows a list of the last ten locations of the iOS device. Although these locations are also displayed in other tabs, this list provides a faster and a better overview.

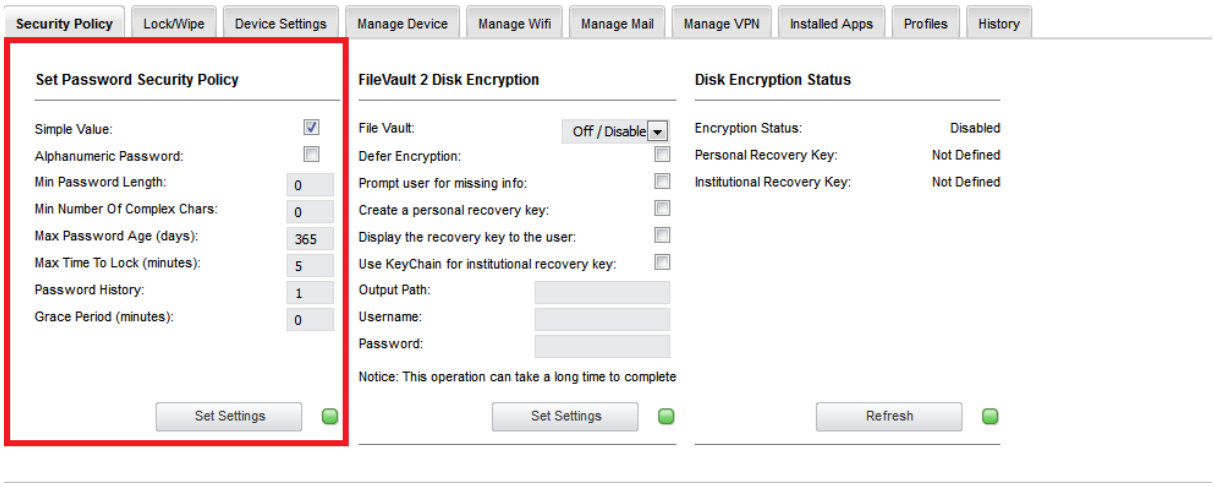


10. Manage OSX Devices

For each operating system (iOS, OS X and Android) different Device Management features are supported and available. . For OS X the different management settings are stored as different profiles. One OS X device can have multiple profiles stored on it.

10.1. Security Settings (Security Profile) on OS X

Enforcing the use of a password / passcode is the most important feature on any device, company or individually owned. Protecting access to data on the device is the first task to protect your OS X devices.



10.1.1. Password / Passcode Setting on OS X Device

Mobile Devices > Security Policy > Set Password Security Policy

The following Settings can be applied for the password / passcode settings for an OS X device:

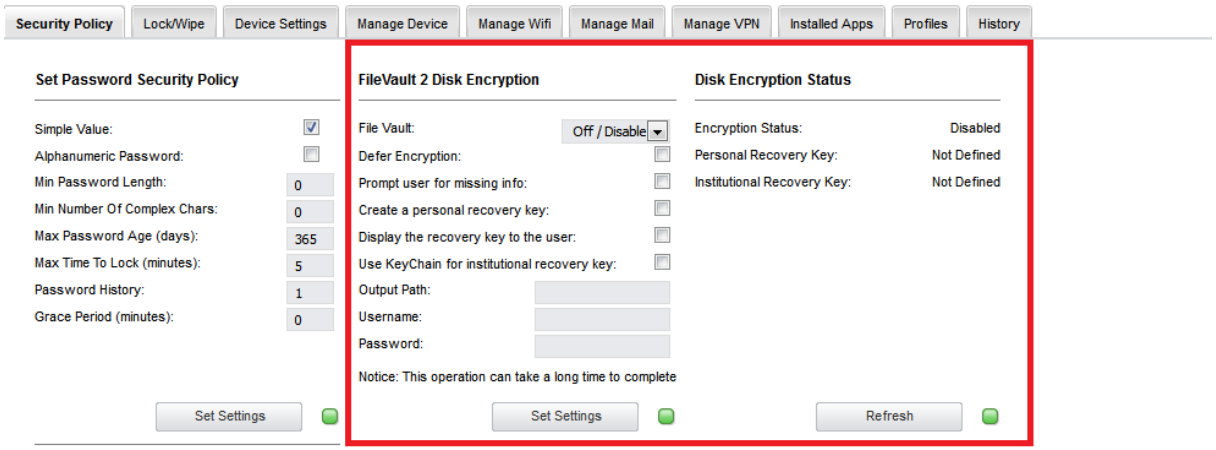
- **Simple Value** – Example Password could be 1221
- **Alphanumeric Password** – Example could be 123A
- **Min Password Length** – Minimum number of digits
- **Min Number Of Complex Chars** – Minimum number of complex characters. Complex characters are for example: !@#$%&* etc.
- **Max Password Age (days)** – Number of days for which a user can use the same password. After that the user is requested to change the password to a new password.
- **Max Time To Lock (minutes)** – If the OS X device is not used the device will lock (request password to access again) after set number of minutes.
- **Password History** – When a new password is set a new password is required. For example, if set to two, it means that after changing the password the user cannot reuse a previously used password until he has set two new passwords in the meantime.
- **Grace Period (minutes)** – Means the time a user has to make a change to the password or to initially set a password after the device receives the security policy.

10.1.2. OS X Device Hardware Encryption

When the password/code for an OS X device is set the OS X device is automatically using it's built in hardware encryption in order to protect data on the device in case it is lost or stolen. We recommend setting a complex password in the security policy in order to have maximum protection.

10.2. File Vault 2 Disk Encryption on OS X

With FileVault 2 you can encrypt the contents of you entire drive to help keep your data secure using XTS-AES 128 encryption.



Here are some guidelines on how to use the FileVault 2 Disk Encryption:

The first step is to change the "File Vault" dropdown to "On/Enable" status. Then there are a few options that can be selected below. Let's take a walk through these buttons and see what each one means.

Defer Encryption – it will defer the encryption until the current user of the Mac will log out.

Prompt user for missing info - in case the administrator did not set the "Password", it will prompt the user to complete, on the device, the missing info.

Create a personal recovery key - FileVault will create a personal key that can be used in case the user password on the device is lost or forgotten, and access is needed to the FileVault encryption.

Display the recovery key to the user – Before starting the encryption the recovery key will be shown to the user, so the user can save it/note it somewhere.

Use Keychain for institutional recovery key- An institutional key will be created and saved at /Library/Keychains/FileVaultMaster.keychain

Output Path – the location on the device where the personal recovery key will be saved

Username – must be an existing user that is already created on the target device

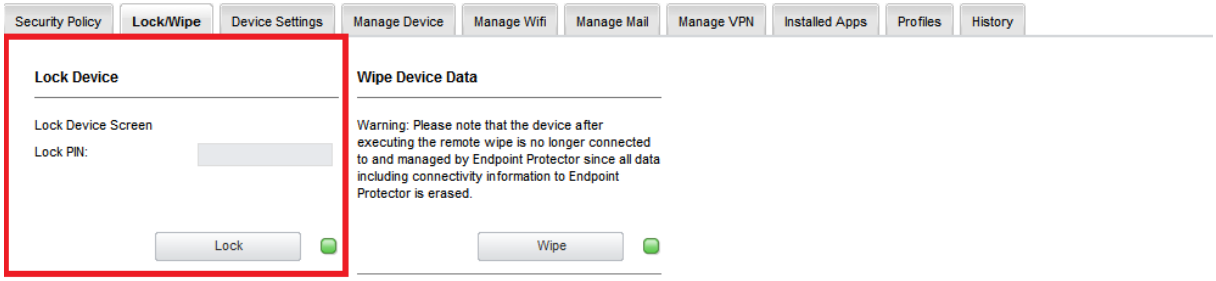
Password – the password for the user.

10.2.1. Disk Encryption Status

FileVault 2 Disk Encryption also has a Status field where it is possible to find information such as the Encryption Status, if the Personal Recover Key was defined or not and if the Institutional Recovery Key was defined or not.

10.3. Remote Lock of Device

Mobile Devices > Lock / Wipe > Lock Device



The OS X device can be remotely locked and a PIN can be set. Clicking "Lock" will remotely lock the device screen and the user will have to enter the PIN to unlock it. The PIN must be a four (4) digit number.

10.4. Remote OS X Device Wipe (Device Nuke)

Mobile Devices > Lock / Wipe > Wipe Device Data

The OS X device can be remotely wiped. A remote wipe will erase all data on the device and reset the device to its factory default. To remotely wipe a device click "Wipe" and a confirmation message will ask to proceed if you are sure you want to remotely wipe the device.

After a remote wipe the device is unmanaged. No more connection between the OS X device and Endpoint Protector is possible after the remote wipe.

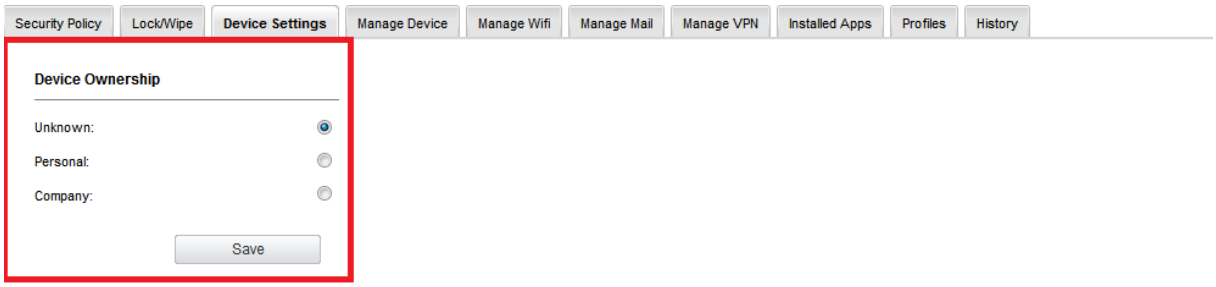
The "Find My Mac PIN" password protects the wiped device. After the device is wiped it will be locked and cannot be used unless the PIN is entered.

Note!

All data on the device will be permanently lost. It cannot be recovered after a remote wipe. Use this feature with caution and only as a last resort, as all existing user's data will be wiped.

10.5. Device Ownership

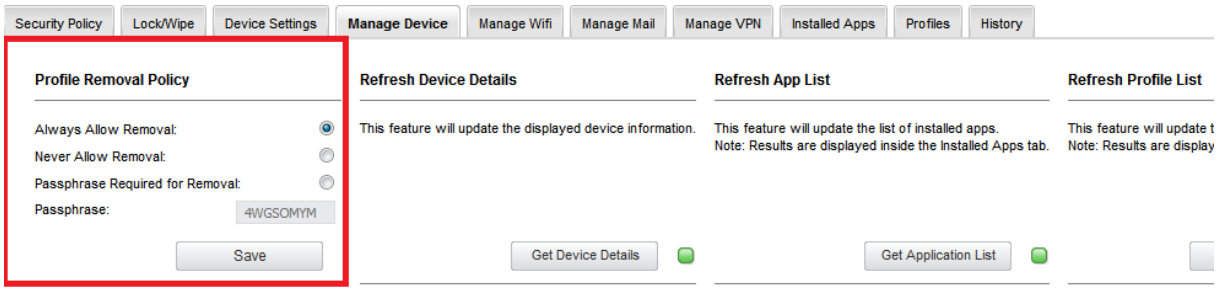
Mobile Devices >Device Settings > Device Ownership



The option "Device Ownership" can be set to who is the rightful owner of a device. Set it to "Company" if the company has purchased the device for the user or to "Personal" if the user has purchased the device and uses it for business purposes. After a device is enrolled the default settings is "Unknown".

10.6. Profile Removal Policy for OS X Devices

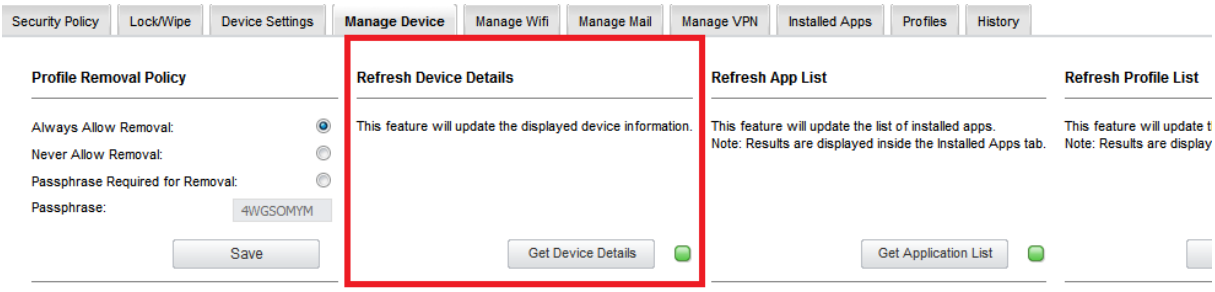
Mobile Devices > Manage Device > Profile Removal Policy



As described in the chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase before the profiles (settings) on an OS X Device can be protected with a passphrase. In this option the passphrase can be changed to be a different one than the one automatically generated and associated with the OTC. For the full description of this option please consult chapter 7.2.2 iOS and OS X Profile Protection Deletion Passphrase.

10.7. Refresh Device Details for OS X

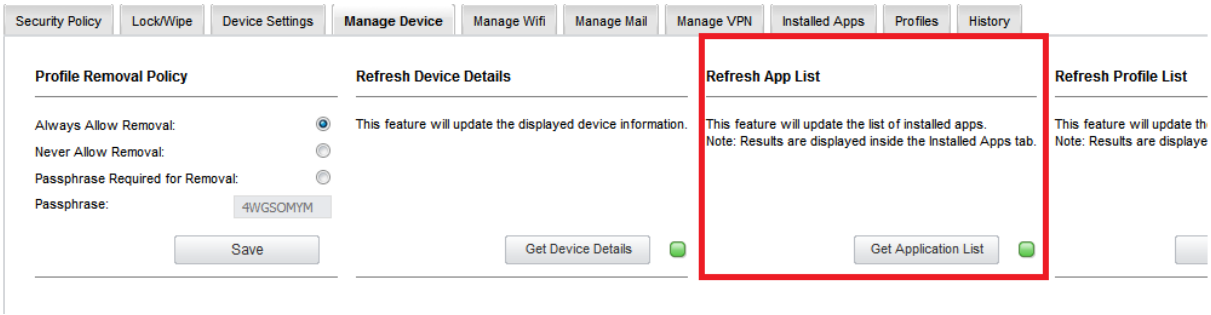
Mobile Devices > Manage Device > Refresh Device Details



This function will ask the OS X devices for its latest details and display them in the Mobile Device Information section.

10.8. Refresh App List for OS X

Mobile Devices > Manage Device > Refresh App List

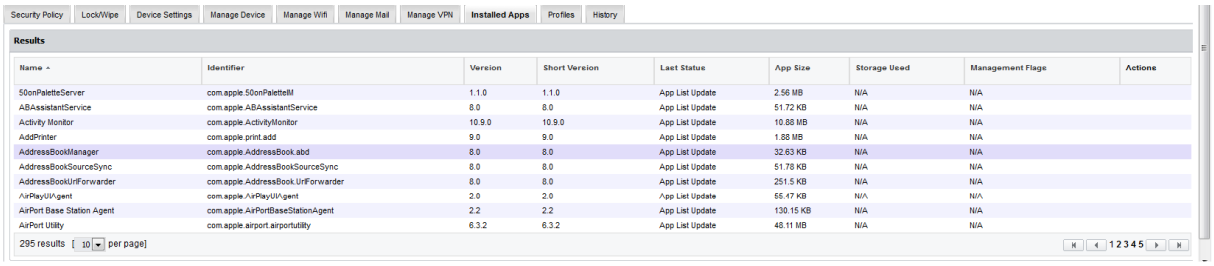


This function by clicking "Get Application List" will ask the OS X device for a list of all the apps installed on the OS X device. The list containing all installed applications will be shown at the "Installed Apps" section. If the user installs a new application, the list of the installed apps will be updated next time when the administrator will request the list of apps by pressing the "Get Application List" button.

10.9. Installed Apps on OS X

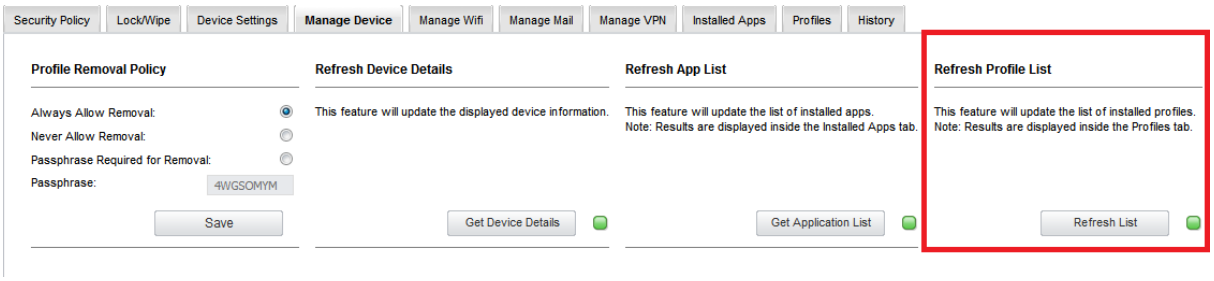
Mobile Devices > Installed Apps

The List of Apps installed on the OS X device lets the Administrator see what apps users have installed on their devices. The list of apps installed on a device can be requested from the OS X device and updated through the option "Get Application List" as described in chapter 10.8 Refresh App List for iOS X.



10.10. Refresh Profile List on OS X

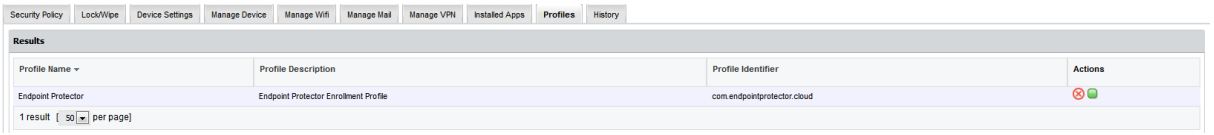
Mobile Devices > Manage Device > Refresh Profile List



The Profile List of an OS X device will show you what profiles are currently installed on the device. The list of installed profiles is shown at Mobile Devices > Profiles.

10.11. Profiles on OS X Devices Information

Mobile Devices > Profiles



The profiles installed on an OS X Device are listed in the "Profiles" tab. There are two types of profile: the main Enrollment Profile and the restriction profiles. The type of profile is shown in the "Profile Description" column. If a new profile is installed on the device, the list of the installed profiles will be updated next time when the administrator will request the list of profiles by pressing the "Get Profiles List" button as described in paragraph 10.10.

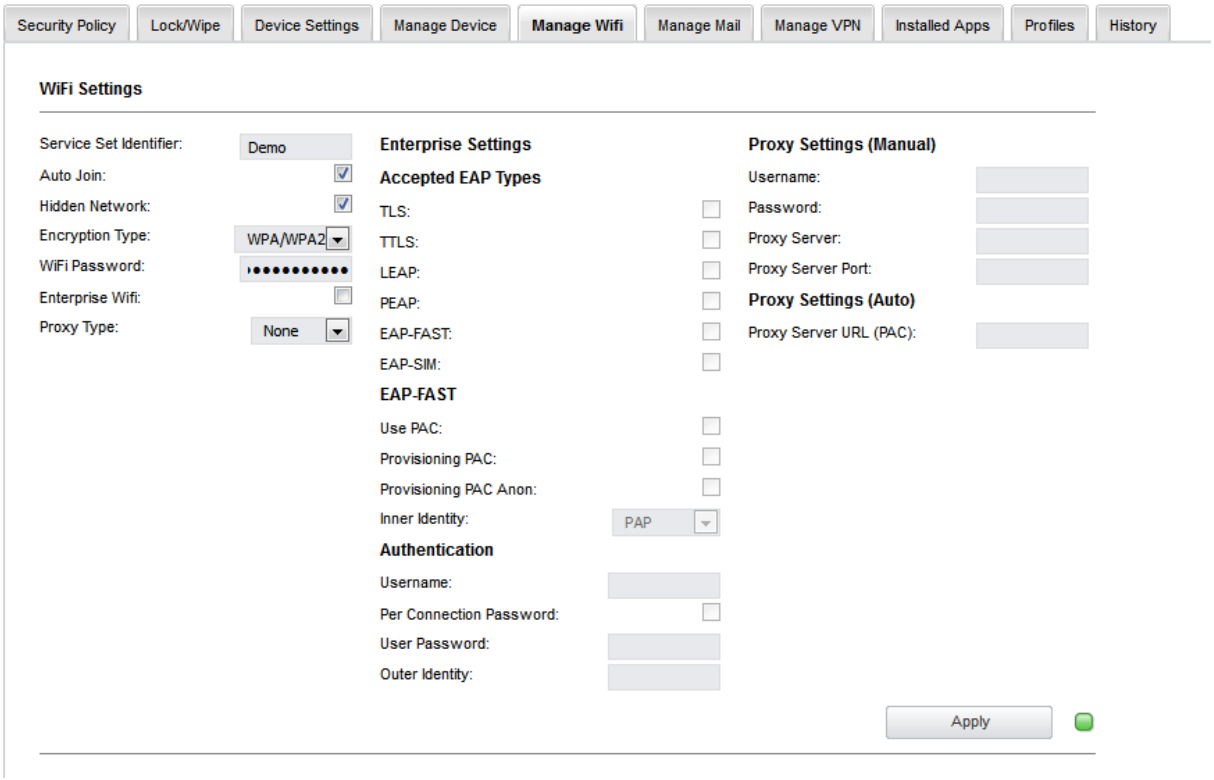
10.11.1. Remove Profile from OS X Device

From here the Endpoint Protector Administrator can also perform the remove action of a profile by clicking on "Remove Profile". If a profile, e.g. a

Restriction Profile is removed, the associated restrictions from the iOS device are removed. In case the Administrator want to unmanage a device, the Enrollment Profile needs to be removed. After removing the enrollment profile the device is no loger managed.

10.12. Manage WiFi on OS X

Mobile Devices > Manage WiFi



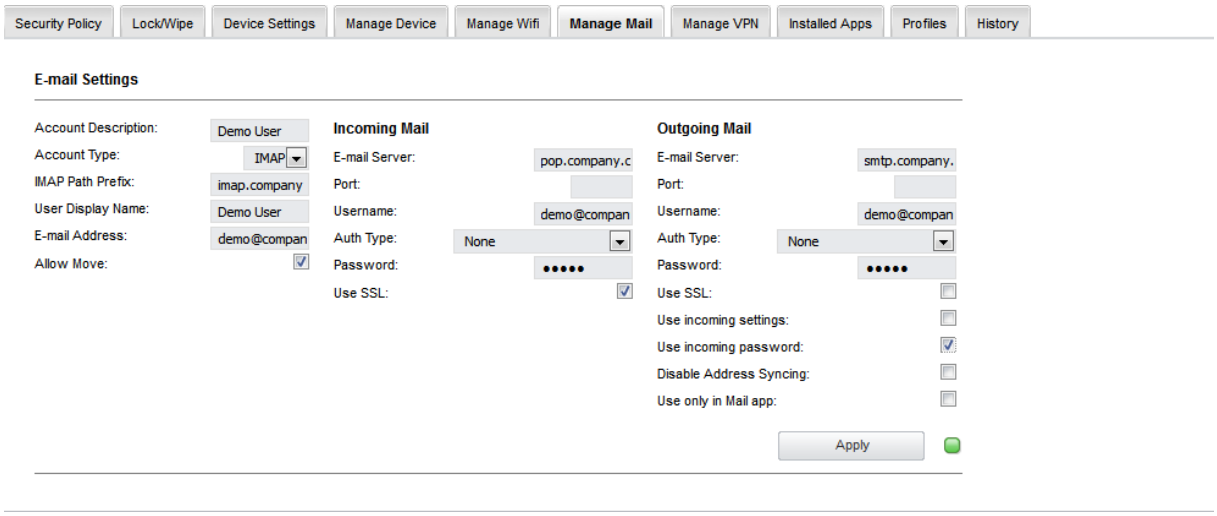
The Endpoint Protector Administrator can apply wireless network (WiFi) settings to an OS X device. This can be used for OS X devices to automatically connect to a WiFi access point without having to manually add the settings on the device.

10.12.1. Wipe Wi-fi Settings

Wi-Fi Profile can be removed to wipe company Wi-Fi Settings while personal Wi-Fi content remains untouched.

10.13. Manage Mail on OS X

Mobile Devices > Manage Mail



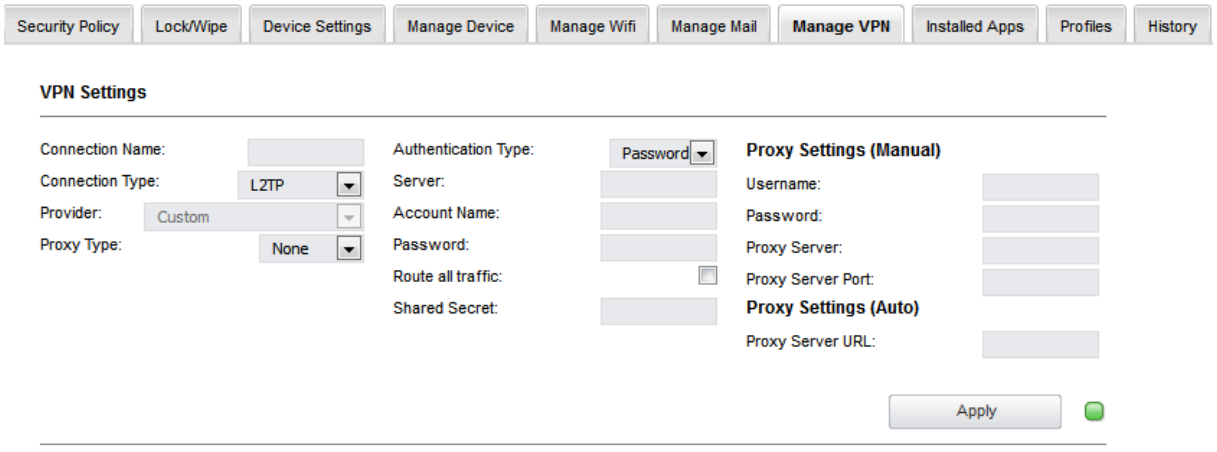
The Endpoint Protector Administrator can apply E-Mail settings to an OS X device. This can be used for OS X devices to automatically use company e-mail accounts and settings without having to manually add the settings on the device.

10.13.1. Wipe E-mail Settings

E-mail Profile can be removed to wipe company E-Mail Content and Settings while personal E-mail accounts and content remain untouched.

10.14. Manage VPN on OS X

Mobile Devices > Manage VPN



The Endpoint Protector Administrator can apply VPN settings to an OS X device. This can be used for OS X devices to automatically deploy and use company VPN settings and policies without having to manually add the settings on the device.

10.15. History of OS X Devices Actions

Mobile Devices > History

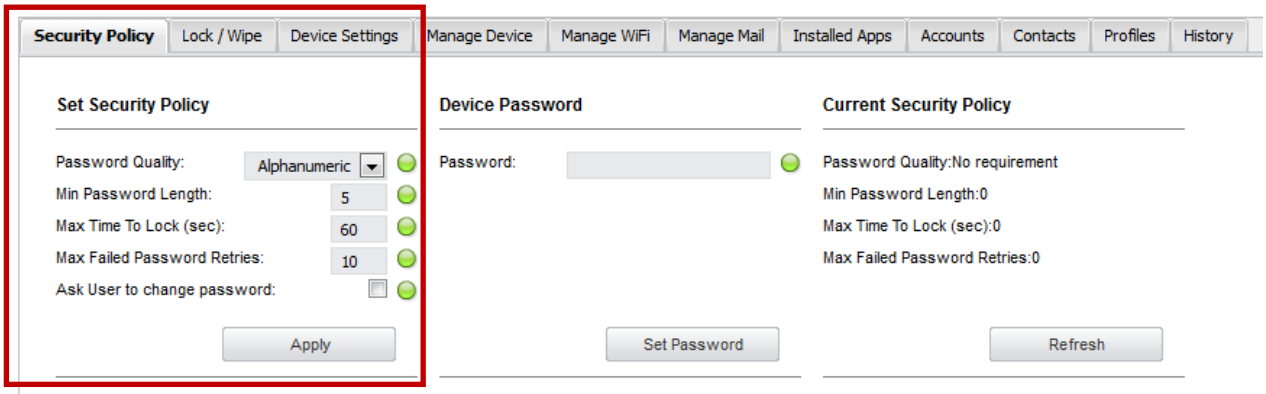
In the “History” tab a record of actions sent to an OS X device are saved and the corresponding results are shown as well. The result can be executed, error, failed or pending.

11. Manage Android Devices

For each operating system (iOS, OS X and Android) different Device Management features are supported and available. For Android the different management settings are enforced by the EPP Client on the Android device.

11.1. Security Settings (Security Profile) on Android

Enforcing the use of a password / passcode is the most important feature on any device, company or individually owned. Protecting access to data on the device is the first task to protecting your Android devices.



The current Security Policy (if any) will be shown on under „Current Security Policy".

11.1.1. Password / Passcode Setting on Android Device

Mobile Devices > Security Policy > Set Security Policy

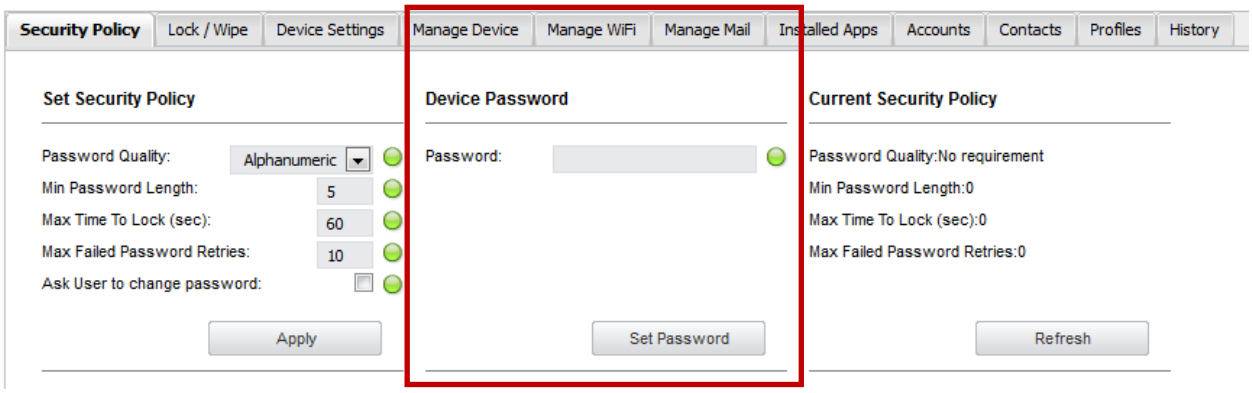
The following Settings can be applied for the password / passcode settings for an Android device:

- **Password Quality** – The following settings can be chosen from:
    - **No requirement**
    - **Any**
    - **Numeric**
    - **Alphabetical**
    - **Alphanumeric**
    - **Complex**
- **Min Password Length** – Minimum number of digits
- **Max Time To Lock (seconds)** – If Android device is not used the device will lock (request password to access again) after set number of seconds.
- **Max Failed Password Retries** –Means the number a user can enter a wrong password until the device will wipe all data and reset itself. In case of reset, the device is wiping its entire data and is reset to a factory default. All data on the device is erased and cannot be recovered.
- **Ask User to change password** – Checking this option will prompt the device user to change from current password to a new password.

To apply the password Policy to the device, make the selection and click “Apply”.

11.1.2. Device Password

Mobile Devices > Security Policy > Device Password



The Administrator can set a password and send it to the Android device. This is helpful in case a user has forgotten the device password or the device screen does not accept user input and the device password has to be changed or set to zero.

To apply the device password to the device make the selection and click "Set Password".

11.1.3. Android Device Hardware Encryption

When the password/passcode for an Android device which has Android Version 4+ is set the Android device is automatically using its build in hardware encryption in order to protect data on the device in case it is lost or stolen. We recommend setting a complex password in the security policy in order to have maximum protection. Earlier Android devices with older versions of Android do not offer this functionality.

11.2. Request Storage Encryption

The administrator can request the Android device's owner/user to encrypt the storage of the device by pressing "Enable Encryption".

.

A message on the device will request the encryption. The request must be accepted, then the encryption type must be chosen (quick or normal). The encryption can be started only if the following requirements are met:

- Complex password to be set
- At least 80% battery remaining on the device

After these steps the encryption will start and the device cannot be used until the encryption is finished.

Note!

The data on the SD Cards will not be encrypted!

11.3. Remote Android Lock of Device

Mobile Devices > Lock / Wipe > Lock Device

The Android device can be remotely locked. Clicking "Lock" will remotely lock the device screen and require a password entry to unlock the screen.

The device can be locked with the current password being kept "Lock Device Screen (Keep Current Password)" or alternatively be locked with a random password if selected "Strong Password Lock (Set Random Password).

The remote lock of a device works also in case of a device that has a SIM card and the SIM card has been removed from the device. As long as the device has a working internet connection, in this case over Wi-Fi the remote locking of the device will still work as long as the lock command can reach the device.

11.4. Remote Android Device Wipe (Device Nuke)

Mobile Devices > Lock / Wipe > Wipe Device Data

Security Policy
Lock / Wipe
Device Settings
Manage Device
Manage WiFi
Manage Mail
Installed Apps
Accounts
Contacts
Profiles
History
Lock Device
Strong Password Lock (Set Random Password)
Lock Device Screen (Keep Current Password)
Lock
Wipe Device Data
Warning: Please note that the device after executing the remote wipe is no longer connected to and managed by Endpoint Protector since all data including connectivity information to Endpoint Protector is erased.
Including SD Card
Wipe
Wipe SD-Card
Warning: this feature will delete all data from SD-Card in the device.
Wipe SD-Card

The Android device can be remotely wiped. A remote wipe will erase all data on the device and reset the device to its factory default. To remotely wipe a device click "Wipe" and a confirmation message will ask to proceed if you are sure you want to remotely wipe the device.

Additionally to wiping the data on the actual device the option to "Include SD Card" can be selected to also wipe the data on an SD Card in the device.

After a remote wipe the device is unmanaged. No more connection between the Android device and Endpoint Protector is possible after the remote wipe.

The remote wipe of a device works also in case of a device that has a SIM card and the SIM card has been removed from the device. As long as the device has a working internet connection, in this case over Wi-Fi the remote wipe of the device will still work as long as the wipe command can reach the device.

Note!

All data on the device will be permanently lost. It cannot be recovered after a remote wipe. Use this feature with caution and only as a last resort.

11.4.1. Android Remote Wipe of SD-Card

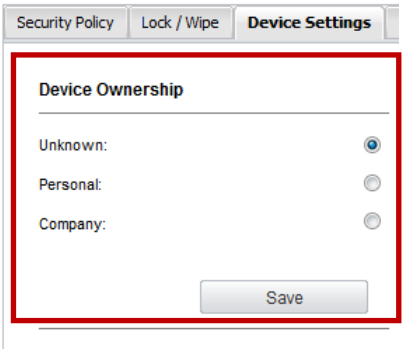
Mobile Devices > Lock / Wipe > Wipe SD-Card

Security Policy
Lock / Wipe
Device Settings
Manage Device
Manage WiFi
Manage Mail
Installed Apps
Accounts
Contacts
Profiles
History
Lock Device
Strong Password Lock (Set Random Password)
Lock Device Screen (Keep Current Password)
Lock
Wipe Device Data
Warning: Please note that the device after executing the remote wipe is no longer connected to and managed by Endpoint Protector since all data including connectivity information to Endpoint Protector is erased.
Including SD Card
Wipe
Wipe SD-Card
Warning: this feature will delete all data from SD-Card in the device.
Wipe SD-Card

The SD Card in an Android device can be remotely wiped using this feature. To wipe the SD Card click "Wipe SD-Card".

11.5. Device Ownership

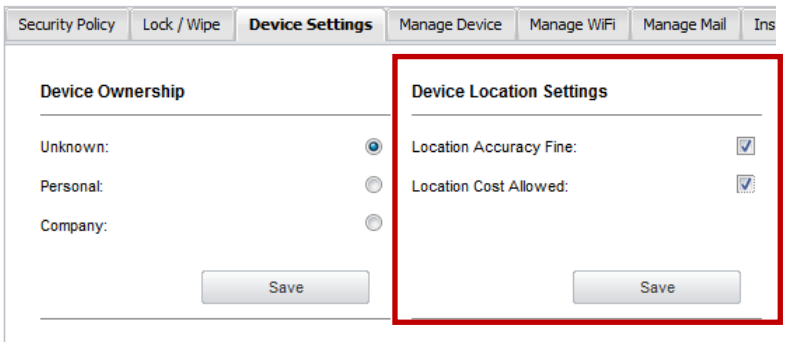
Mobile Devices >Device Settings > Device Ownership



The option "Device Ownership" can be set to who is the rightful owner of a device. Set it to "Company" if the company has purchased the device for the user or to "Personal" if the user has purchased the device and uses it for business purposes. After a device is enrolled the default settings is set to "Unknown".

11.6. Android Device Location Settings

Mobile Devices >Device Settings > Device Location Settings



These settings impact the acuaracy of the location data used to locate an Android device.

11.6.1. Location Accuracy Fine on Android

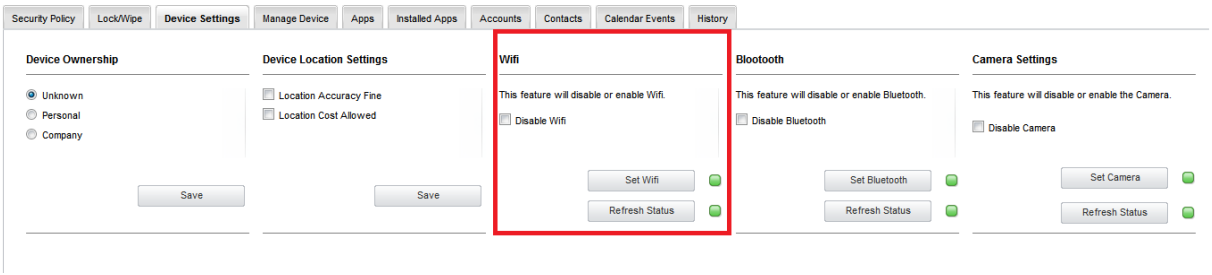
The setting "Location Accuracy Fine" unchecked relies on data from WiFi or triangulation. Checked "Location Accuracy Fine" will rely on GPS data.

11.6.2. Location Cost Allowed on Android

The setting "Location Cost Allowed" will send location data even if device is outside of the regular network.

11.7. Manage Wifi

This feature will enable or disable the Wifi on the Android device.

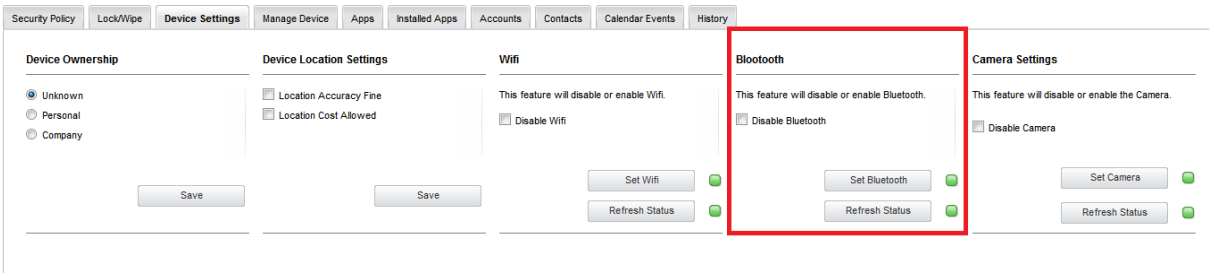


Note!

Make sure that you have a valid internet connection (other than Wifi) otherwise the communication between the EPP Server and the Android devices will not be possible!

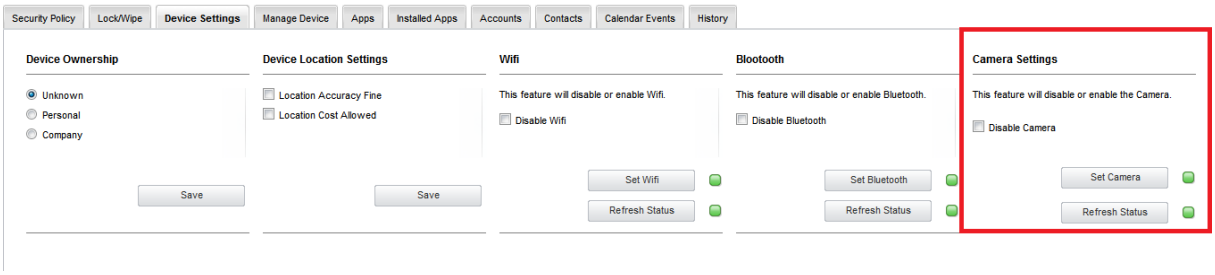
11.8. Manage Bluetooth

This feature will enable or disable the Bluetooth on the Android device.



11.9. Manage Camera on Android

This feature can disable the camera of the Android device.



11.10. Play Sound on Device for Android

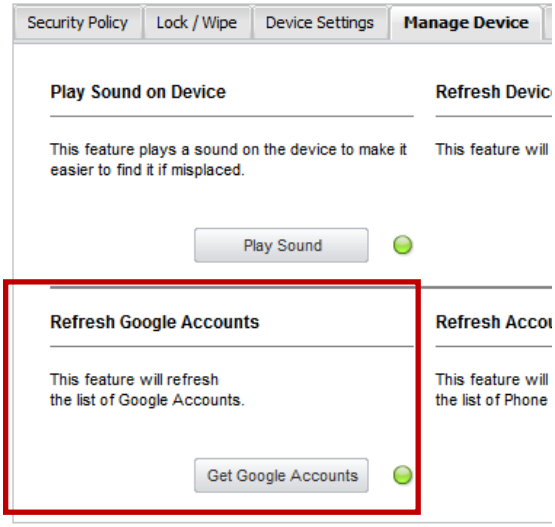
Mobile Devices >Manage Device > Play Sound on Device

Security Policy
Lock / Wipe
Device Settings
Manage Device
Play Sound on Device
This feature plays a sound on the device to make it easier to find it if misplaced.
Play Sound

The option "Play Sound" will make the Android device play a loud noise in order to locate a misplaced device.

11.11. Refresh Google Accounts for Android

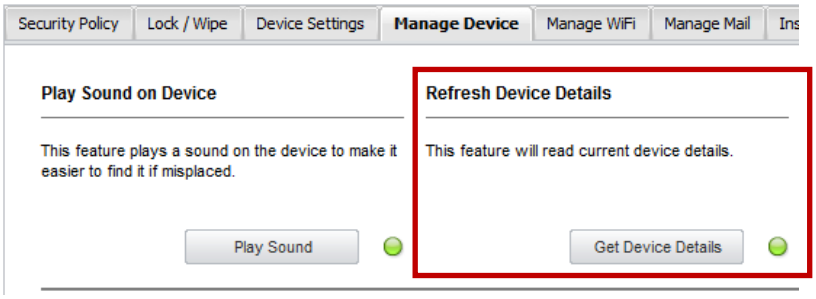
Mobile Devices >Manage Device > Refresh Google Accounts


Security Policy
Lock / Wipe
Device Settings
Manage Device
Play Sound on Device
This feature plays a sound on the device to make it easier to find it if misplaced.
Play Sound
Refresh Google Accounts
This feature will refresh the list of Google Accounts.
Get Google Accounts

The option Refresh Google Accounts by clicking "Get Google Accounts" will receive a list of Google accounts registered with the Android device. The list of Accounts is displayed under Mobile Devices >Manage Device > Accounts.

11.12. Refresh Device Details for Android

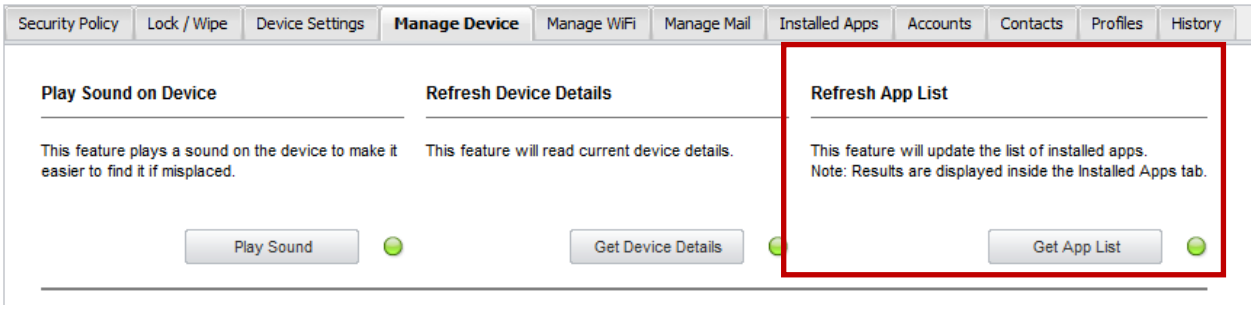
Mobile Devices > Manage Device > Refresh Device Details


Security Policy
Lock / Wipe
Device Settings
Manage Device
Manage WiFi
Manage Mail
Play Sound on Device
This feature plays a sound on the device to make it easier to find it if misplaced.
Play Sound
Refresh Device Details
This feature will read current device details.
Get Device Details

This function will ask the Android devices for its latest details and display them in the Mobile Device Information section. This function is particularly useful if all device information is not displayed after enrollment.

11.13. Refresh App List for Android

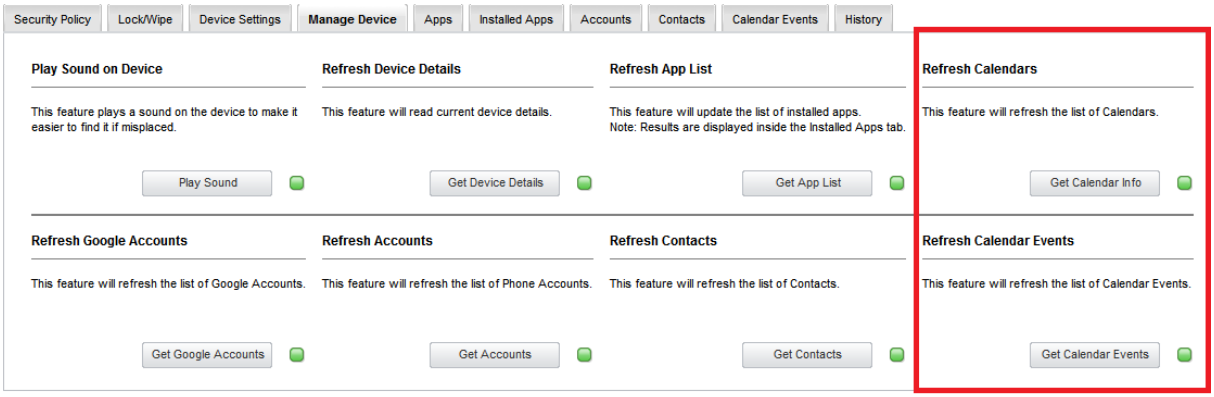
Mobile Devices > Manage Device > Refresh App List



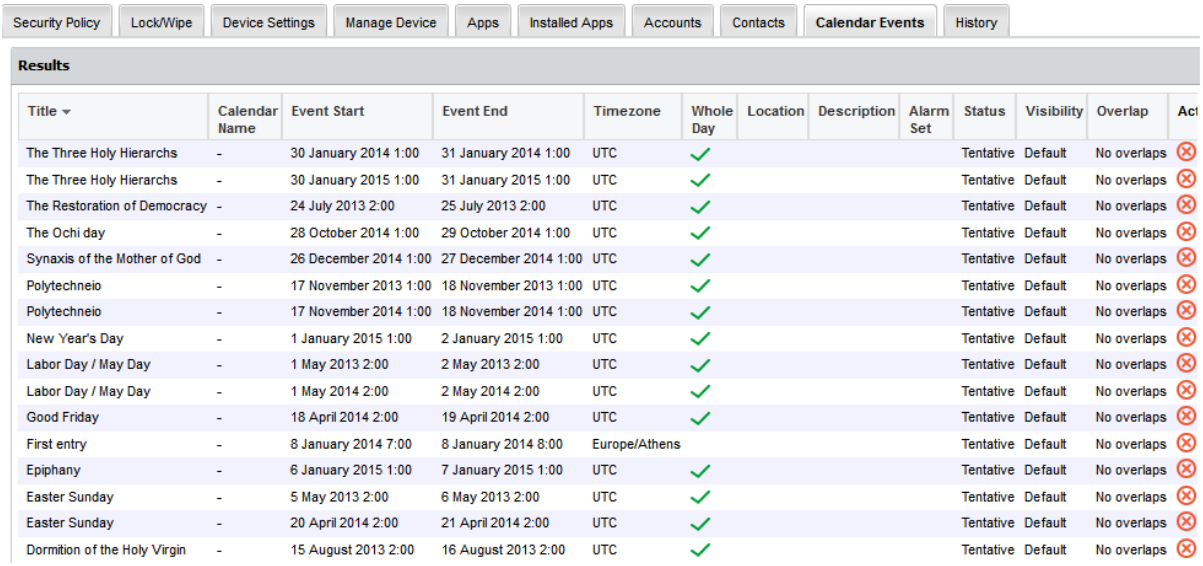
This function by clicking "Get App List" will ask the Android device for a list of all the apps installed on the Android device. The list of all installed Apps is shown in Endpoint Protector MDM at
Mobile Devices > Installed Apps

11.14. Manage Calendar Events

Through this feature it is possible to manage the Calendar Events on an Android device. The list of the existing events can be requested by pushing the "Get Calendar Info" and "Get Calendar Events" buttons.


Security Policy
Lock/Wipe
Device Settings
Manage Device
Apps
Installed Apps
Accounts
Contacts
Calendar Events
History
Play Sound on Device
This feature plays a sound on the device to make it easier to find it if misplaced.
Play Sound
Refresh Device Details
This feature will read current device details.
Get Device Details
Refresh App List
This feature will update the list of installed apps.
Note: Results are displayed inside the Installed Apps tab.
Get App List
Refresh Calendars
This feature will refresh the list of Calendars.
Get Calendar Info
Refresh Google Accounts
This feature will refresh the list of Google Accounts.
Get Google Accounts
Refresh Accounts
This feature will refresh the list of Phone Accounts.
Get Accounts
Refresh Contacts
This feature will refresh the list of Contacts.
Get Contacts
Refresh Calendar Events
This feature will refresh the list of Calendar Events.
Get Calendar Events

The administrator will see the events in the "Calendar Events" section. In the screenshot below we did not push the "Get Calendar Info" button, so only the "Calendar Events" are listed (note that the "Calendar Name" field is empty). If we would push the button afterwards, the "Calendar Name" field would also get completed.

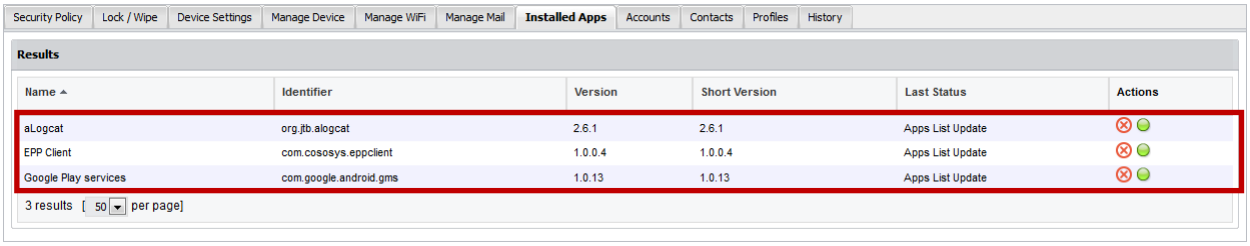


Title	Calendar Name	Event Start	Event End	Timezone	Whole Day	Location	Description	Alarm Set	Status	Visibility	Overlap	Act
The Three Holy Hierarchs	-	30 January 2014 1:00	31 January 2014 1:00	UTC	✓				Tentative	Default	No overlaps	
The Three Holy Hierarchs	-	30 January 2015 1:00	31 January 2015 1:00	UTC	✓				Tentative	Default	No overlaps	
The Restoration of Democracy	-	24 July 2013 2:00	25 July 2013 2:00	UTC	✓				Tentative	Default	No overlaps	
The Ochi day	-	28 October 2014 1:00	29 October 2014 1:00	UTC	✓				Tentative	Default	No overlaps	
Synaxis of the Mother of God	-	26 December 2014 1:00	27 December 2014 1:00	UTC	✓				Tentative	Default	No overlaps	
Polytechneio	-	17 November 2013 1:00	18 November 2013 1:00	UTC	✓				Tentative	Default	No overlaps	
Polytechneio	-	17 November 2014 1:00	18 November 2014 1:00	UTC	✓				Tentative	Default	No overlaps	
New Year's Day	-	1 January 2015 1:00	2 January 2015 1:00	UTC	✓				Tentative	Default	No overlaps	
Labor Day / May Day	-	1 May 2013 2:00	2 May 2013 2:00	UTC	✓				Tentative	Default	No overlaps	
Labor Day / May Day	-	1 May 2014 2:00	2 May 2014 2:00	UTC	✓				Tentative	Default	No overlaps	
Good Friday	-	18 April 2014 2:00	19 April 2014 2:00	UTC	✓				Tentative	Default	No overlaps	
First entry	-	8 January 2014 7:00	8 January 2014 8:00	Europe/Athens					Tentative	Default	No overlaps	
Epiphany	-	6 January 2015 1:00	7 January 2015 1:00	UTC	✓				Tentative	Default	No overlaps	
Easter Sunday	-	5 May 2013 2:00	6 May 2013 2:00	UTC	✓				Tentative	Default	No overlaps	
Easter Sunday	-	20 April 2014 2:00	21 April 2014 2:00	UTC	✓				Tentative	Default	No overlaps	
Dormition of the Holy Virgin	-	15 August 2013 2:00	16 August 2013 2:00	UTC	✓				Tentative	Default	No overlaps	

11.15. Installed Apps on Android

Mobile Devices > Installed Apps

The List of Apps installed on the Android device lets the Administrator see what apps users have installed on their devices. The list of apps installed on a device can be requested from the Android device and updated though the option "Get App List" as described in chapter 11.13 Refresh App List for Android.



Name	Identifier	Version	Short Version	Last Status	Actions
aLogcat	org.jtb.alogcat	2.6.1	2.6.1	Apps List Update	
EPP Client	com.cososys.eppclient	1.0.0.4	1.0.0.4	Apps List Update	
Google Play services	com.google.android.gms	1.0.13	1.0.13	Apps List Update	

3 results [50 per page]

In future versions of Endpoint Protector MDM more features for managing apps on Android devices will be introduced.

11.15.1. Removing Installed Apps on Android

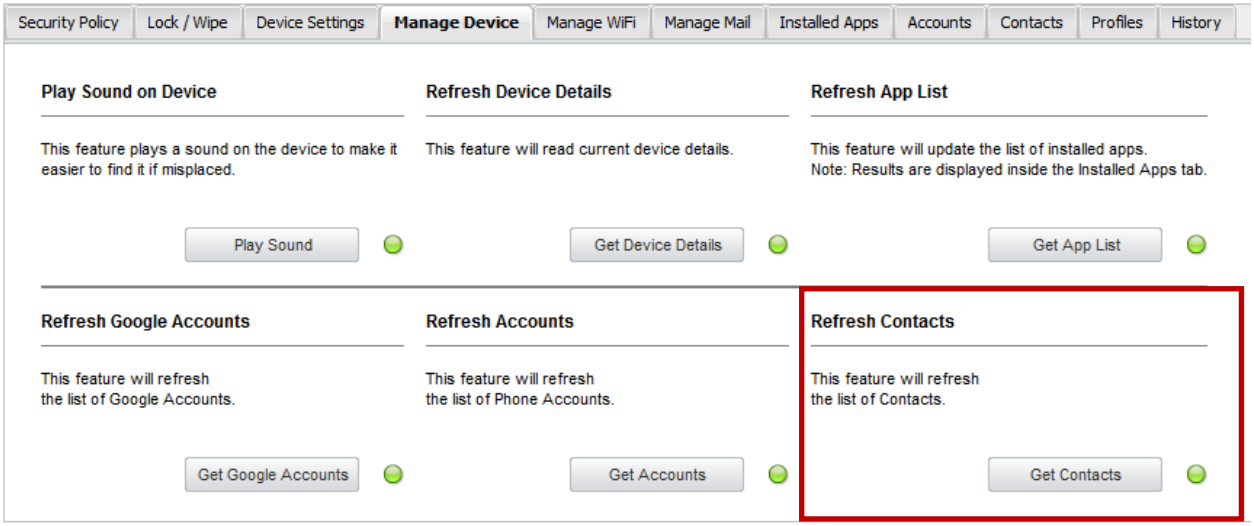
The Endpoint Protector Administrator can send an action to the Android device and ask the device to remove the app from the device. By clicking the ⊗ „Remove App" button the request is sent to the device. The Android device will now show the user that the device is supposed to be removed. The user can oppose removal and simply deny this. In this case the Administrator should send another request for removal. Due to the Androids Operating System, in the current scenario the App cannot be forcefully unistalled.

11.16. Get Contacts on Android

Mobile Devices > Contacts

The tab "Contacts" Lists all contacts that are saved in the address book of an Android device.

To retrieve the list of contacts on the device the Endpoint Protector Administrator can request the list by clicking "Get Contacts" under the option Mobile Devices > Manage Devices > Refresh Contacts.


Security Policy
Lock / Wipe
Device Settings
Manage Device
Manage WiFi
Manage Mail
Installed Apps
Accounts
Contacts
Profiles
History
Play Sound on Device
This feature plays a sound on the device to make it easier to find it if misplaced.
Play Sound
Refresh Device Details
This feature will read current device details.
Get Device Details
Refresh App List
This feature will update the list of installed apps.
Note: Results are displayed inside the Installed Apps tab.
Get App List
Refresh Google Accounts
This feature will refresh the list of Google Accounts.
Get Google Accounts
Refresh Accounts
This feature will refresh the list of Phone Accounts.
Get Accounts
Refresh Contacts
This feature will refresh the list of Contacts.
Get Contacts

11.17. Get Accounts on Android

Mobile Devices > Accounts

The tab "Accounts" Lists all accounts used on an Android device.

To retrieve the list of Accounts on the device the Endpoint Protector Administrator can request the list by clicking "Get Accounts" under the option Mobile Devices > Manage Devices > Refresh Accounts.

11.18. History of Android Device Actions

Mobile Devices > History

In the "History" tab a record of actions send to an Android device are saved and the corresponding results is shown as well. The result can be executed, error, failed or pending.

Htc_europe HTC Wildfire S A510e	SetMaximumTimeToLock	Success		24 October 2012 15:09
Htc_europe HTC Wildfire S A510e	SetMaximumFailedPasswordsForWipe	Success		24 October 2012 15:09
Htc_europe HTC Wildfire S A510e	SetPasswordMinimumLength	Success		24 October 2012 15:09
Htc_europe HTC Wildfire S A510e	SetPasswordQuality	Success		24 October 2012 15:09
Htc_europe HTC Wildfire S A510e	AskUserChangePassword	Success		24 October 2012 15:05
Htc_europe HTC Wildfire S A510e	GetContacts	Success		24 October 2012 15:05
Htc_europe HTC Wildfire S A510e	GetAccounts	Success		24 October 2012 15:04
Htc_europe HTC Wildfire S A510e	GetGoogleAccounts	Success		24 October 2012 15:04
Htc_europe HTC Wildfire S A510e	GetInstalledPackages	Success		24 October 2012 15:04
Htc_europe HTC Wildfire S A510e	GetDeviceInfo	Success		24 October 2012 15:04

11.19. Manage WiFi, Manage Mail, Profiles on Android

Mobile Devices > Manage WiFi

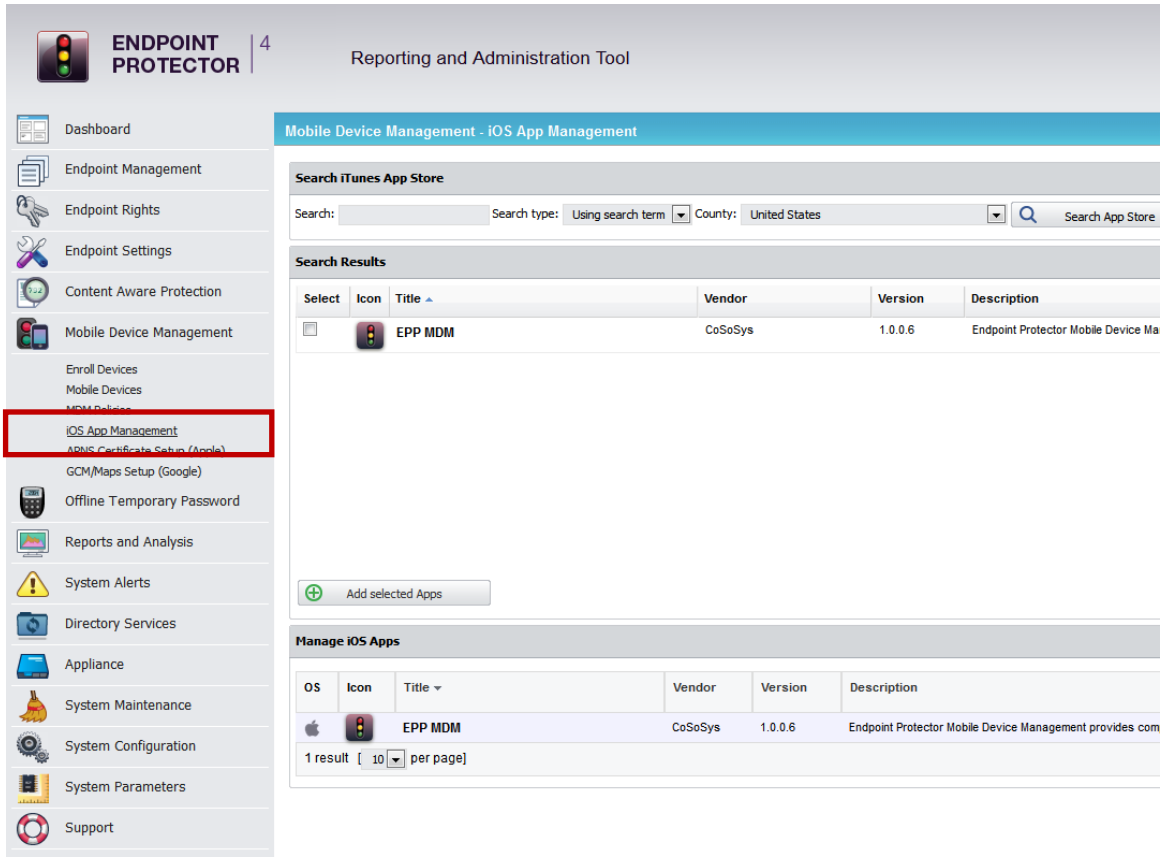
Mobile Devices > Manage Mail

Mobile Devices > Profiles

The tabs “Manage WiFi”, “Manage Mail” and “Profiles” have no functionality associated with them for Android and show “No Results”. This function is currently only supported for iOS devices.

12. Mobile Application Management (MAM) for iOS

The Mobile Application Management (MAM) feature in Endpoint Protector for iOS gives the Endpoint Protector Administrator the power to push Apps from the App store on managed iOS devices. The feature in the current version supports paid and free apps listed on iTunes App Store. (The feature supports paid and free apps listed on iTunes App Store and enterprise apps that are developed "in-house") Mobile Apps can be managed under the following option Mobile Device Management > iOS App Management.

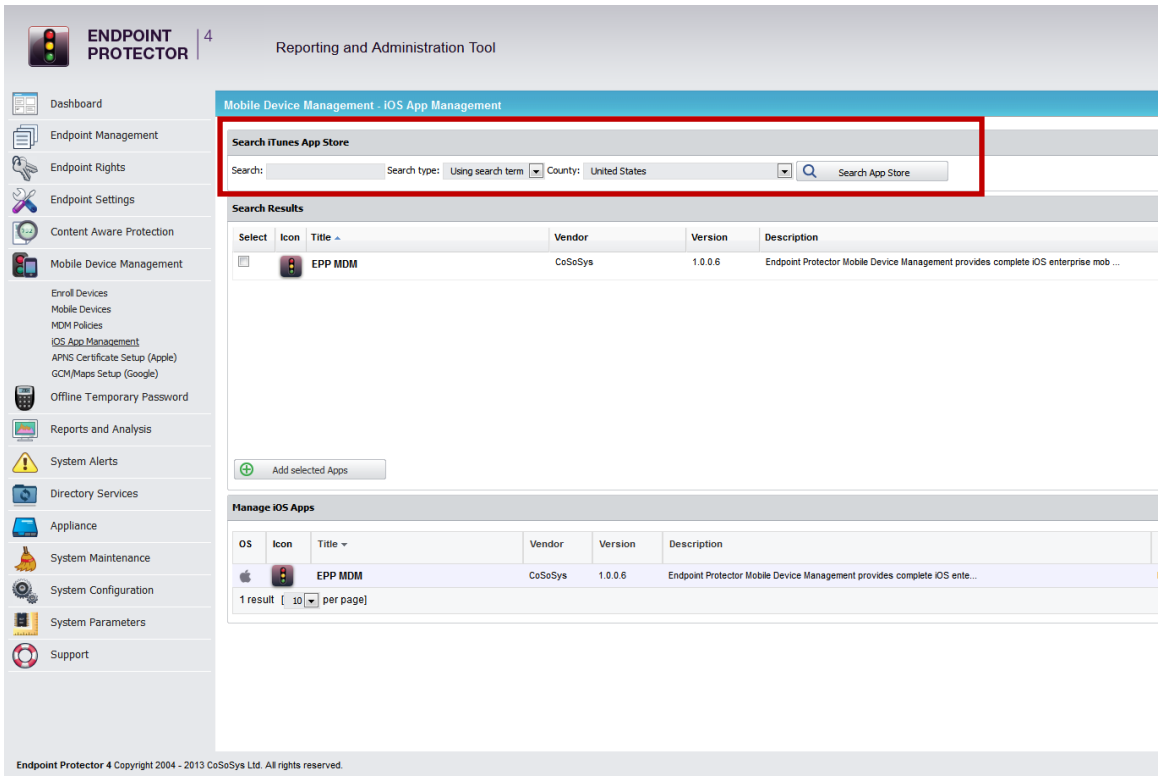


12.1. Adding Apps to your Managed Apps Catalog

To add Apps search for the App in the iTunes App Store directly in the Endpoint Protector interface.

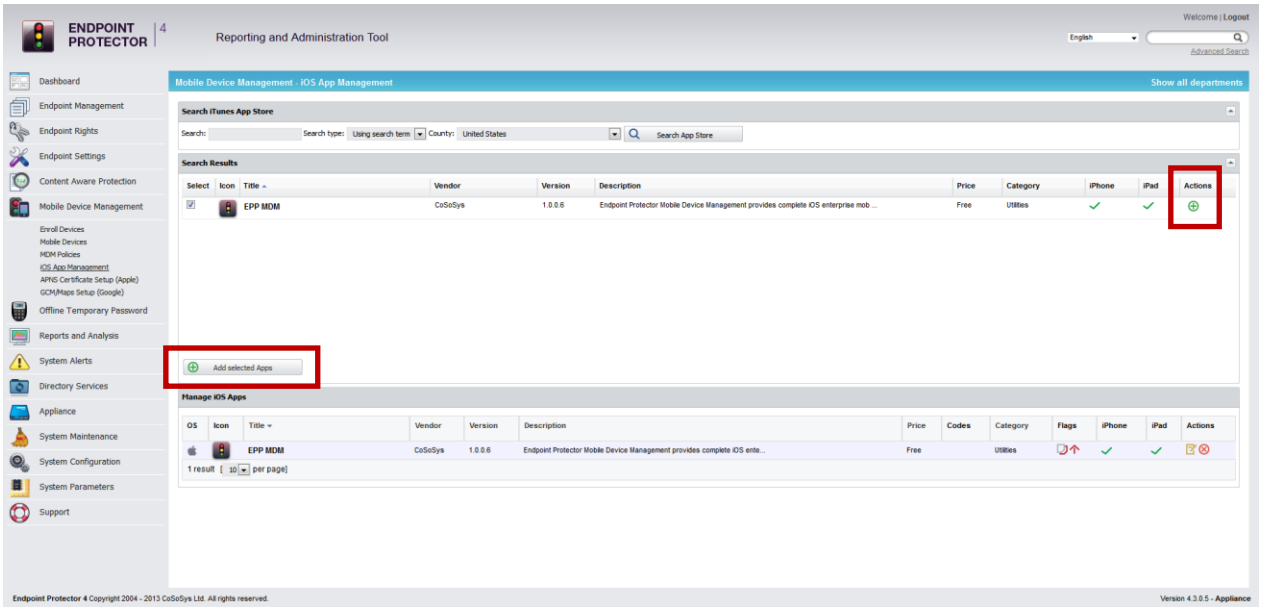
12.1.1. Searching for Apps

Searching for Apps is possible by entering the name of the App or by directly entering the App ID of an App (e.g. the App ID for the EPP MDM iOS App is id570954584). The App ID is stated in the URL of an app when viewing the app details in a web browser
(e.g. https://itunes.apple.com/us/app/epp-mdm/**id570954584**.
For either type of search select "Using search term" or "Using iTunes App ID".



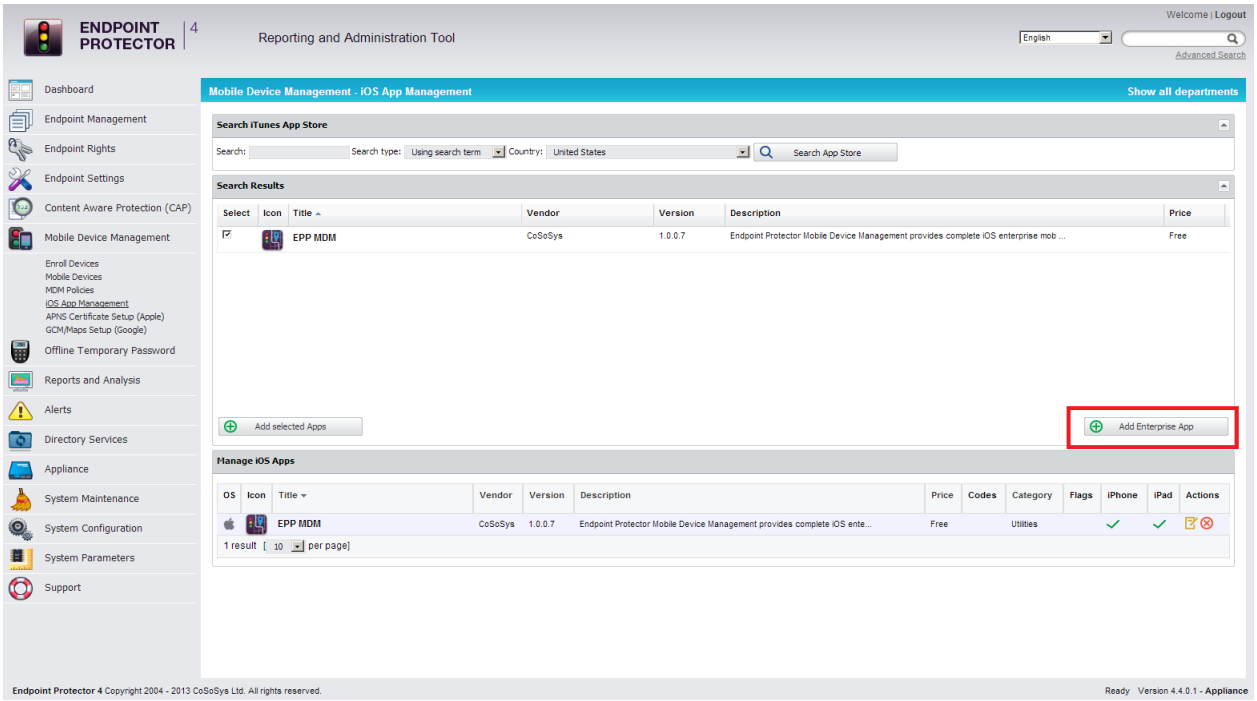
12.1.2. Adding Apps to Managed Apps Catalog

To add an App to your Managed Apps Catalog select the App from the "Search Results" and click "Add selected Apps".

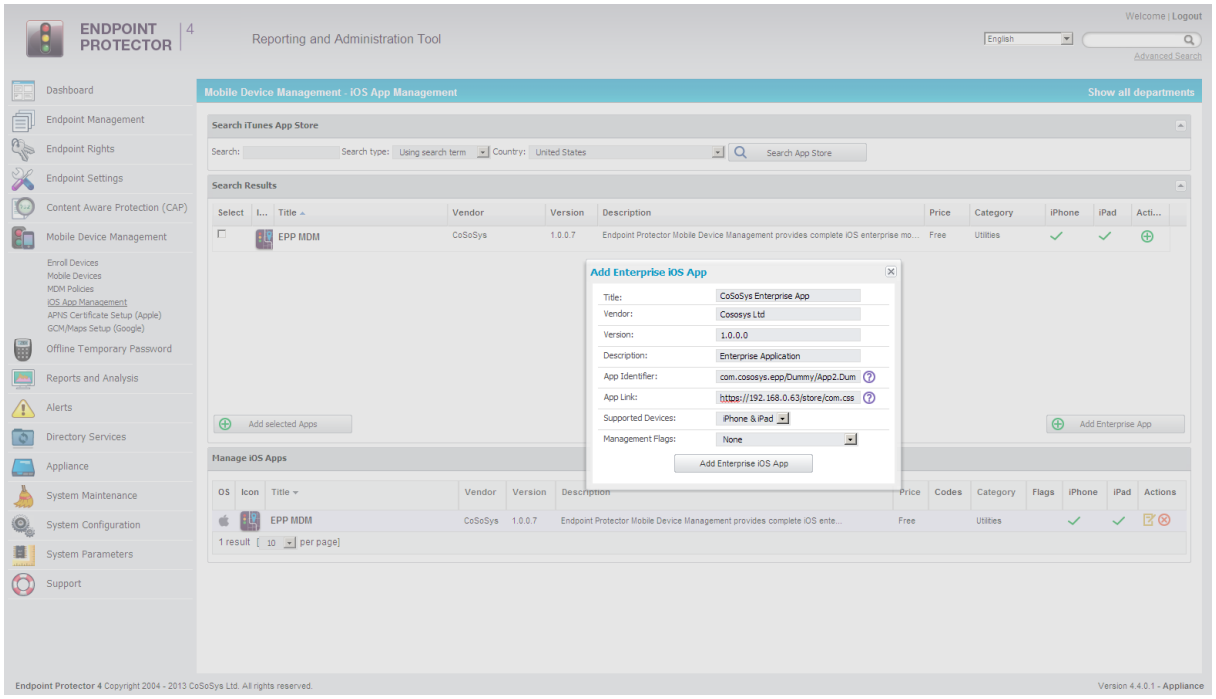


12.1.3. Adding „Enterprise Apps" to Managed Apps Catalog

You can add applications developed „in-house" by clicking on the „Add Enterprise App" button.

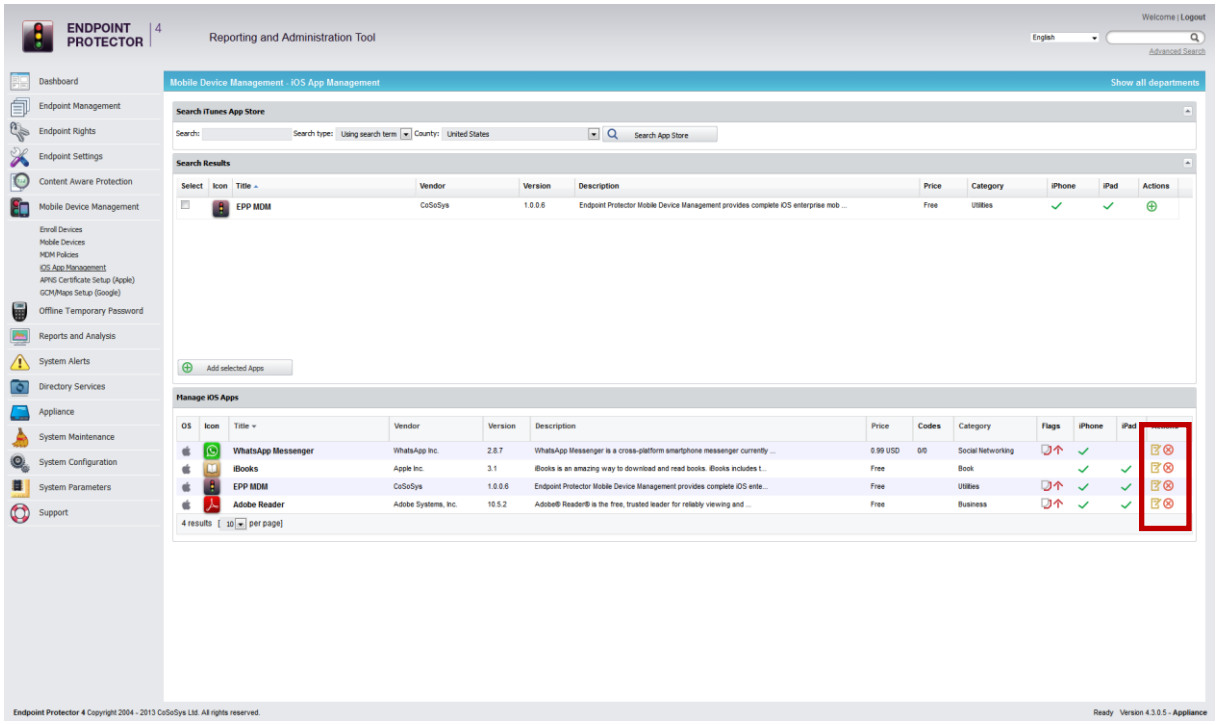


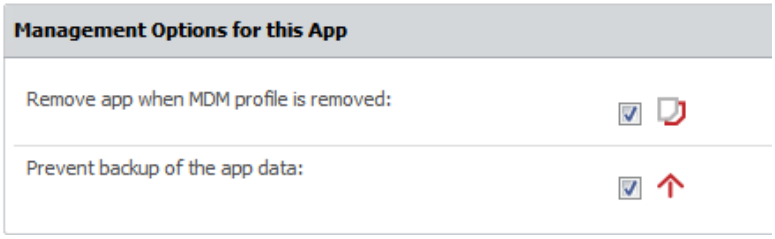
You will have to enter the required details in the pop-up window.



12.2. Editing App Management Options

Managed Apps options can be modified by selecting “Edit App”.

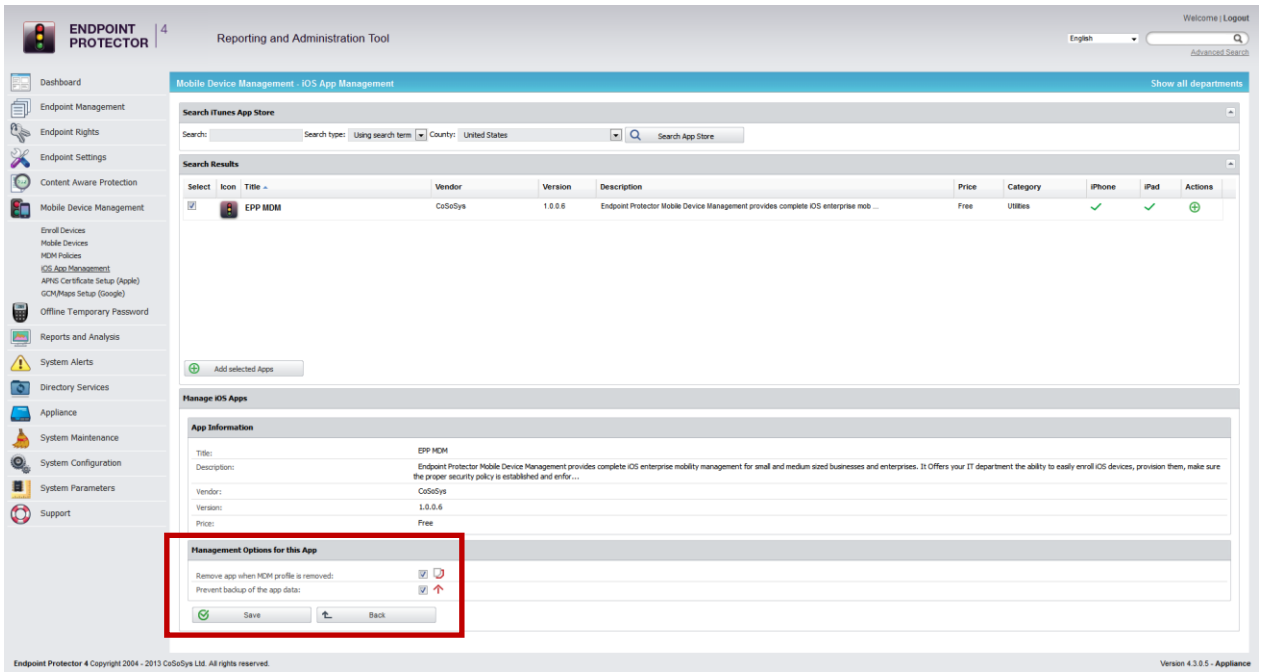




The options for managed Apps are:

- **Remove app when MDM profile is removed**
  if this management flag is set the managed App and all its associated data/content with it, will be removed if the iOS device becomes unmanaged, either if the Endpoint Protector administrator unmanages the device or if the device user is unmanaging the device by removing the device enrollment profile.

- **Prevent backup of the app data**
  if this management flag is set the managed Apps associated data/content will not be backed up in case the device is synced or backed up with iTunes.

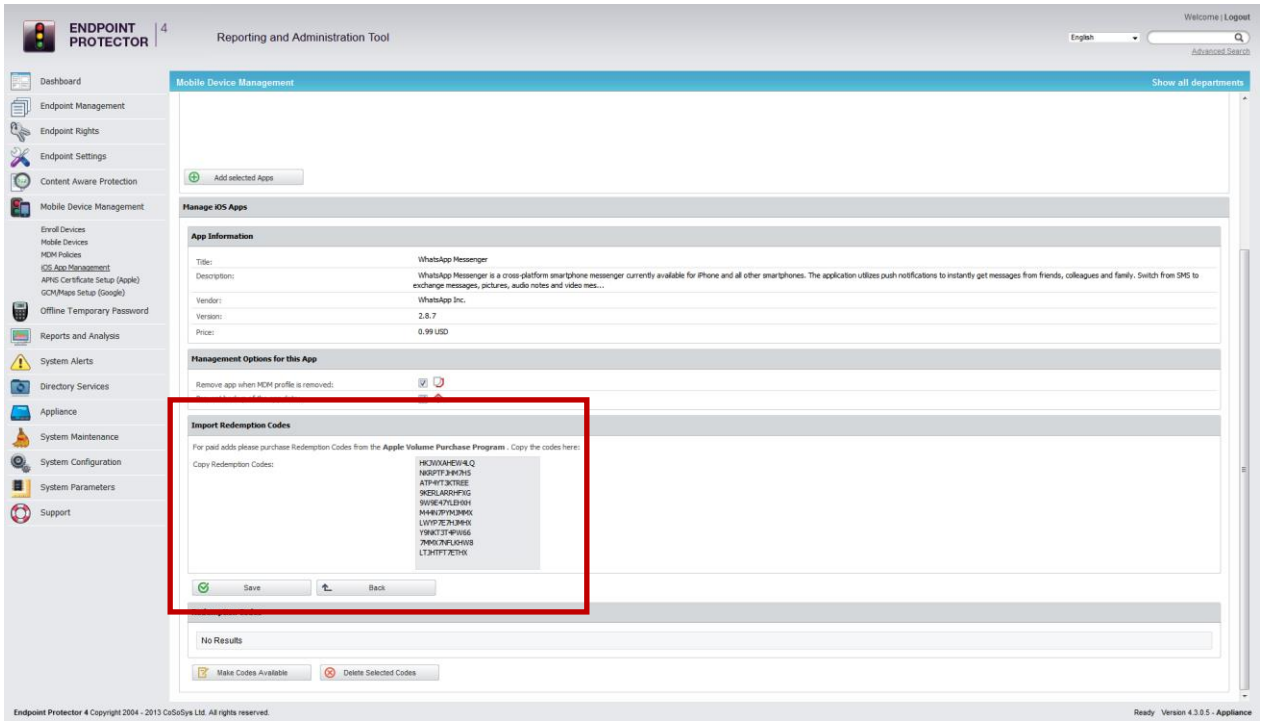


12.3. Managed Paid Apps

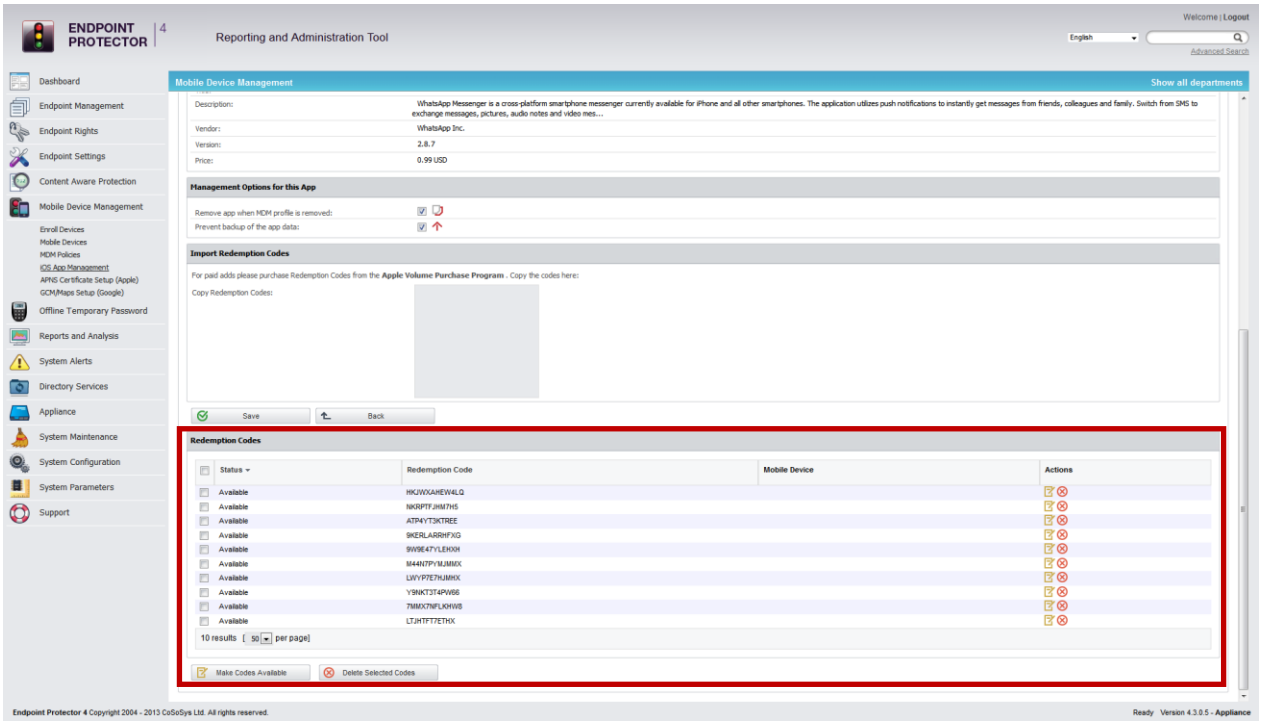
Paid Apps require purchasing license keys through the Apple Volume Purchase Program. The licenses (which Apple calls Redemption Codes) can be purchased here: https://vpp.itunes.apple.com.

This option is available in the Endpoint Protector interface only for paid apps when selecting "Edit App" under the point "Import Redemption Codes".

After redemption codes have been purchased from Apple they need to be introducted through copy/pasting the redeption codes into the Endpoint Protector interface under the option "Edit App" > Import Redemption Codes.

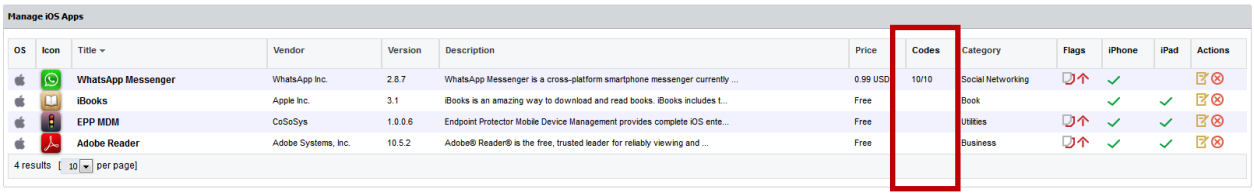


After adding the redemption codes click "Save". The saved redemption codes will be listed under "Edit App" > Redemption Codes.



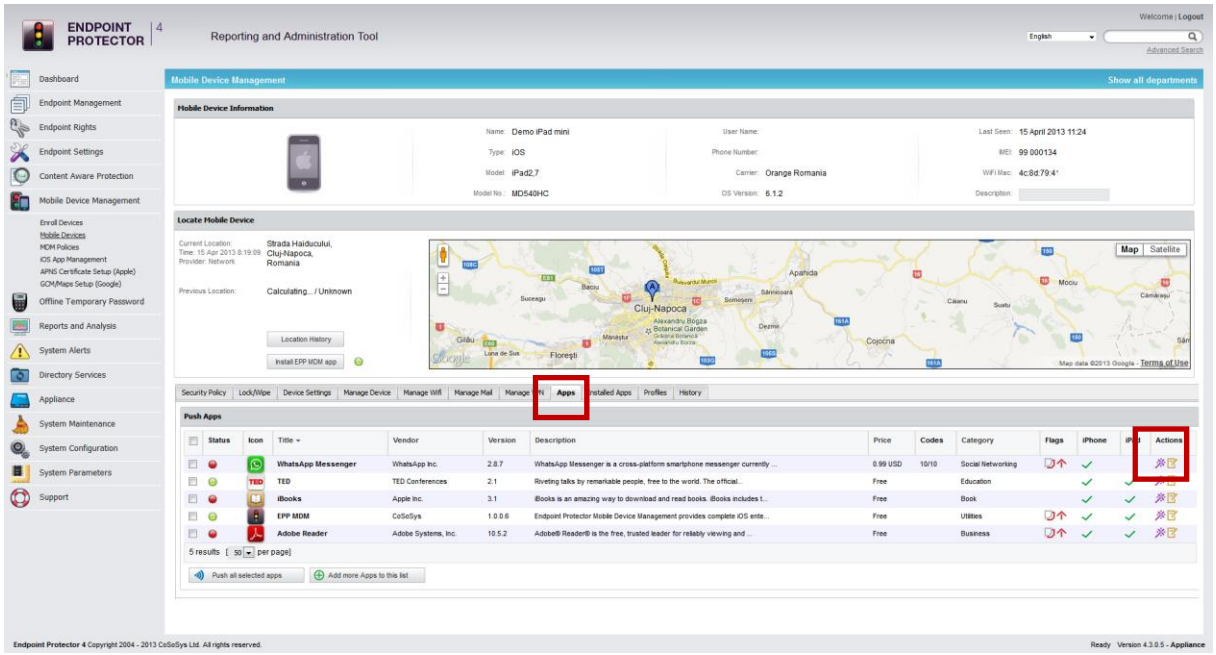
All redemption codes show their status either as available or used in case they have been used, meaning a code was used when a paid app was pushed to a device which did not alreay have this paid app installed.

Additionally the number of total and still available (not yet consumed) redemption codes is shown in the column "Codes" in the list of "Managed iOS Apps". In the example below 10/10 meaning ten of ten codes are available.



12.4. Pushing Apps to iOS Devices

The list of Managed Apps is available when viewing the details about any managed iOS device in the tab “Apps”.



Only Apps that have been added to the Managed App Catalog are displayed in this tab.

To push an app to a managed device click the icon. A message will show that the app has been pushed to the device.

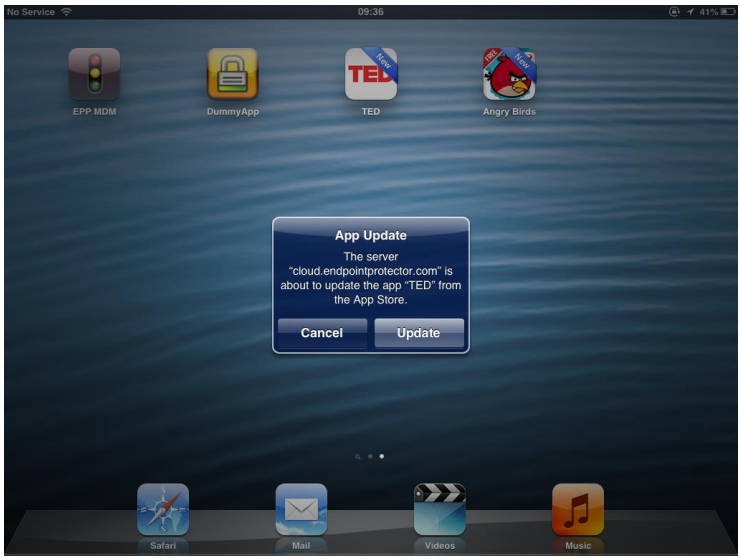
After the app has been pushed to the device the user is prompted to install the app and to provide the iTunes account password associated with the device.

App Installation
The server "cloud.endpointprotector.com" is about to install the app "iBooks" from the App Store.
Your iTunes account will not be charged for this app.
Cancel
Install

Apps can also be pushed from MDM policies “Manage Apps” tab.

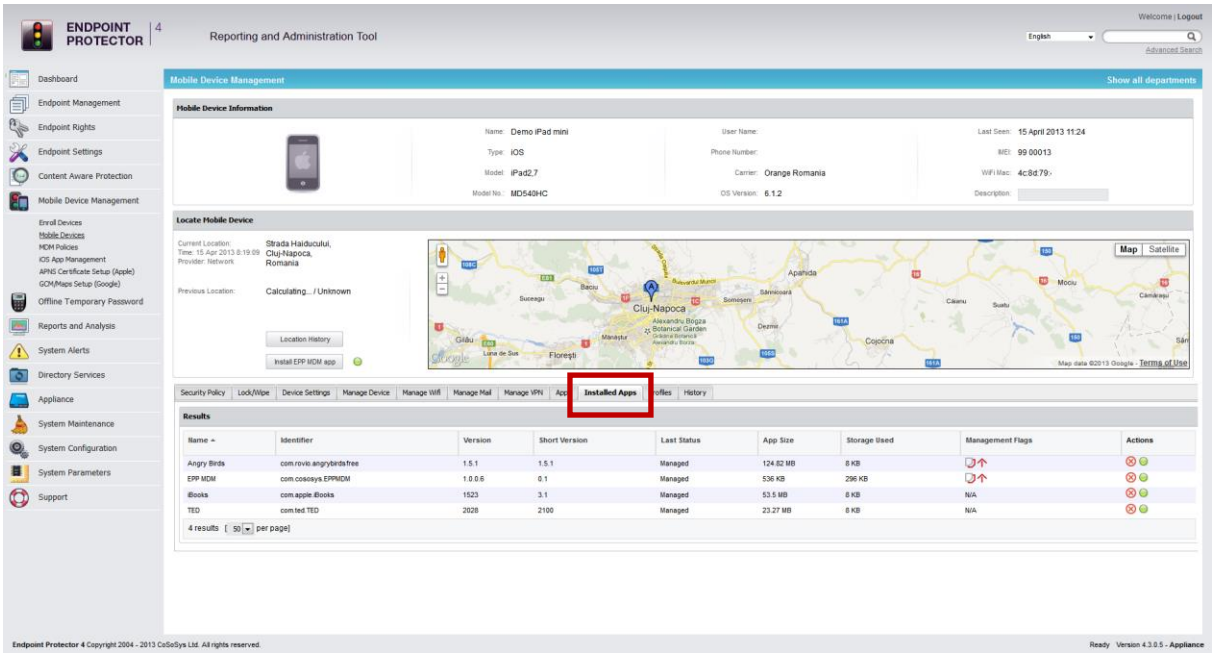
12.4.1. Update Managed Apps / Changing Settings

In case a newer version of an app is available you can update it using the same steps as when pushing a new app to a managed device. In case an update is pushed the user will be prompted to update the app. In case of paid apps no new redemption code is consumed during this process.



12.5. Removing Managed Apps from iOS Devices

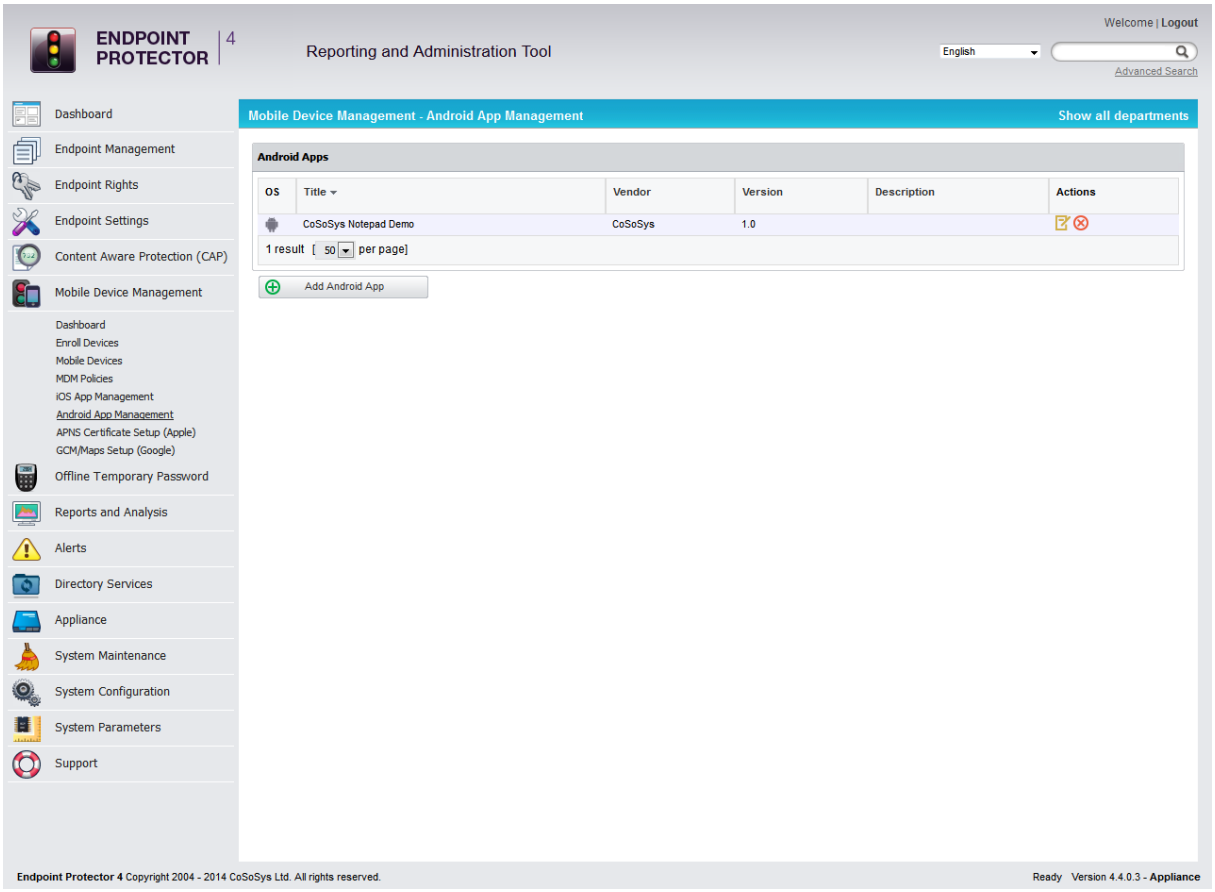
All installed Apps on a managed iOS device are displayed in the tab "Installed Apps".



To remove an app click the icon and the app will be deleted from the managed iOS device. When a managed app is removed on the device the device user is not asked to confirm the removal of the app.

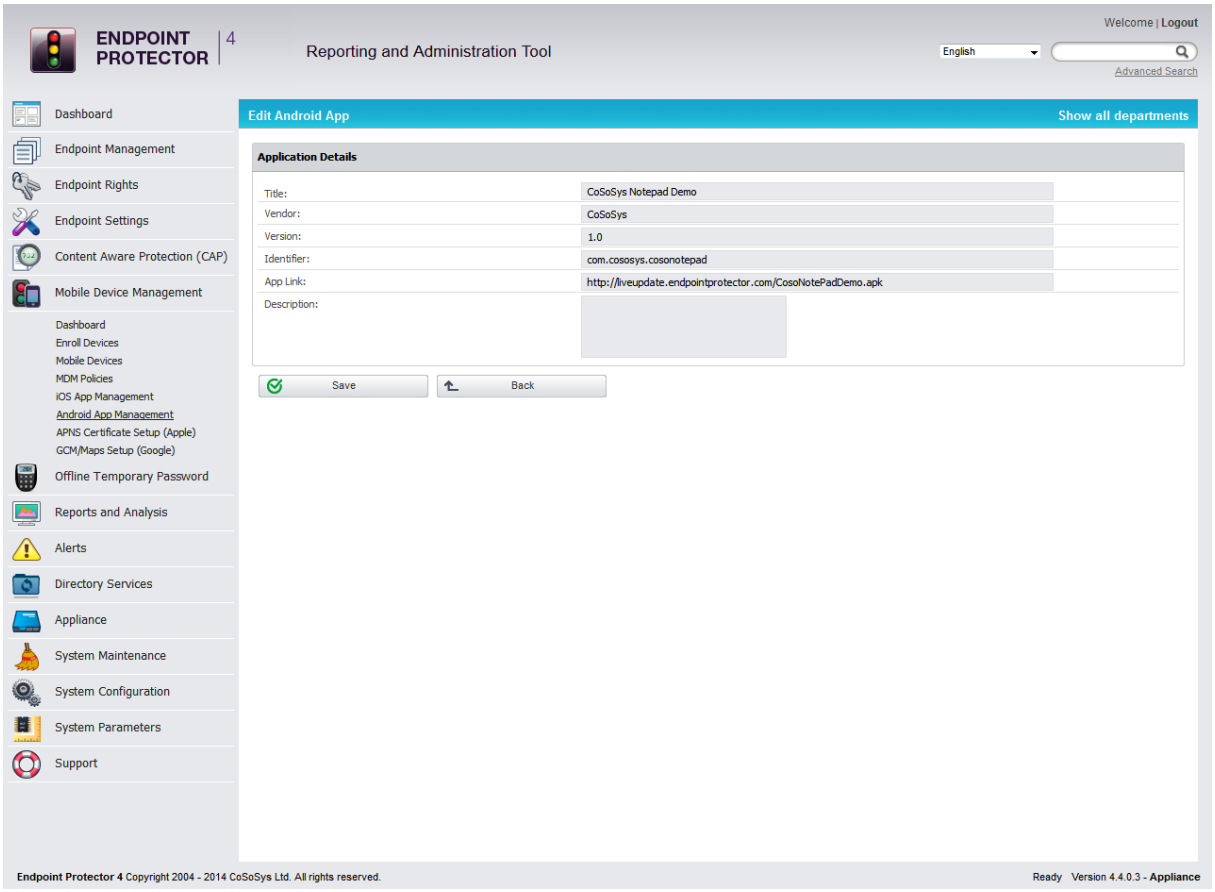
13. Android App Management

The Mobile Application Management (MAM) feature in Endpoint Protector for Android gives the Endpoint Protector Administrator the power to push Apps on managed Android devices. The feature in the current version supports Android apps. Mobile Apps can be managed under the following option Mobile Device Management > Android App Management.



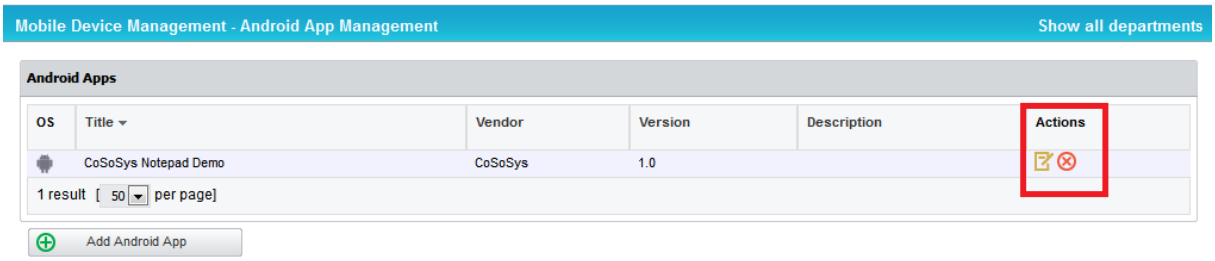
13.1. Adding Apps to your Managed Apps Catalog

To add Apps in the Catalog push the "Add Android App" button, and complete the required fields. The administrator must make the application available on the internet (if it isn't already), then the corresponding link must be entered in the "App Link" field.



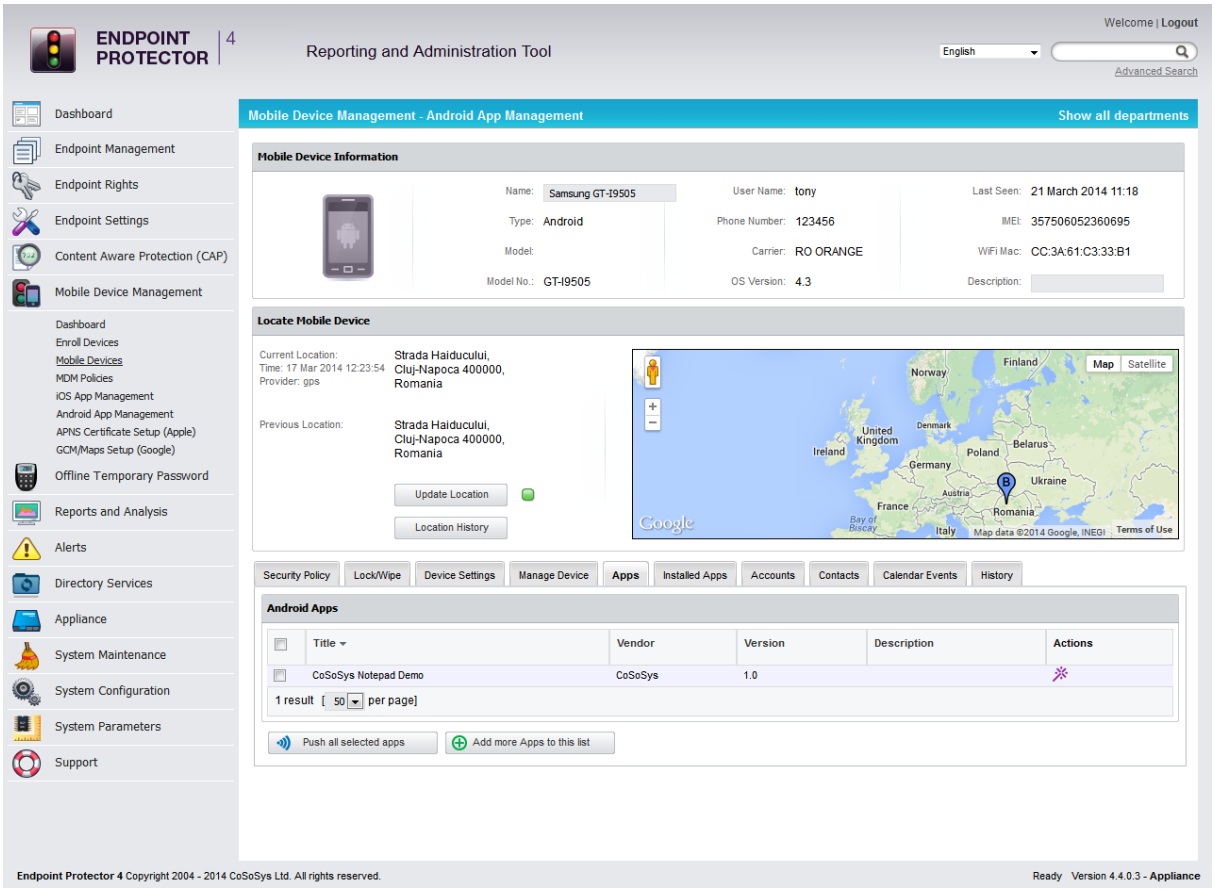
13.2. Editing App Management Options

Managed Apps can be modified by selecting "Edit App" or they can be deleted by pressing the "Delete" button.



13.3. Pushing Apps to Android Devices

The list of Managed Apps is available when viewing the details about any managed Android device in the "Apps" tab.



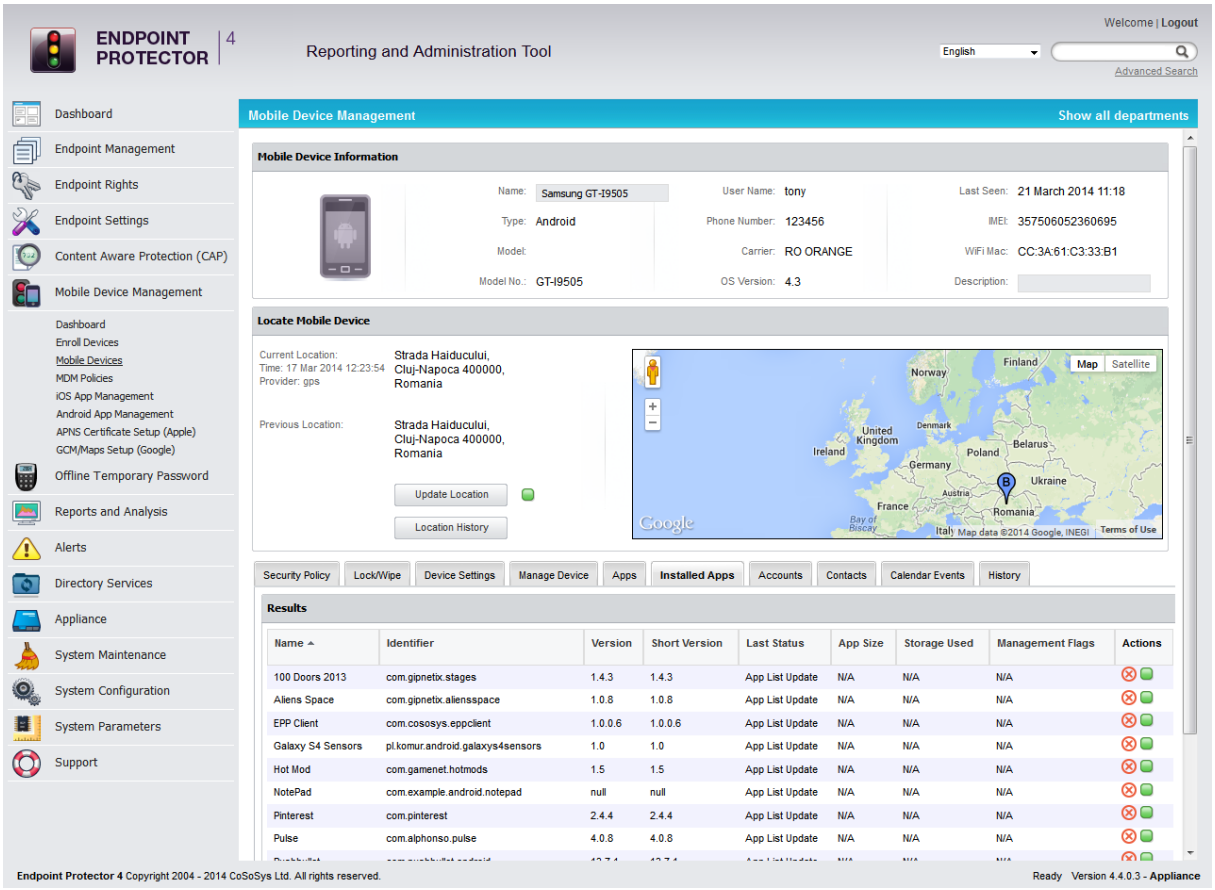
Only Apps that have been added to the "Android App Management" tab are displayed.

To push an app to a managed device click the icon. A message will show that the app has been pushed to the device. Multiple applications can be sent by pressing the "Push all selected apps" button.

Apps can also be pushed from Android policies' "Manage Apps" tab.

13.4. Removing Managed Apps from Android Devices

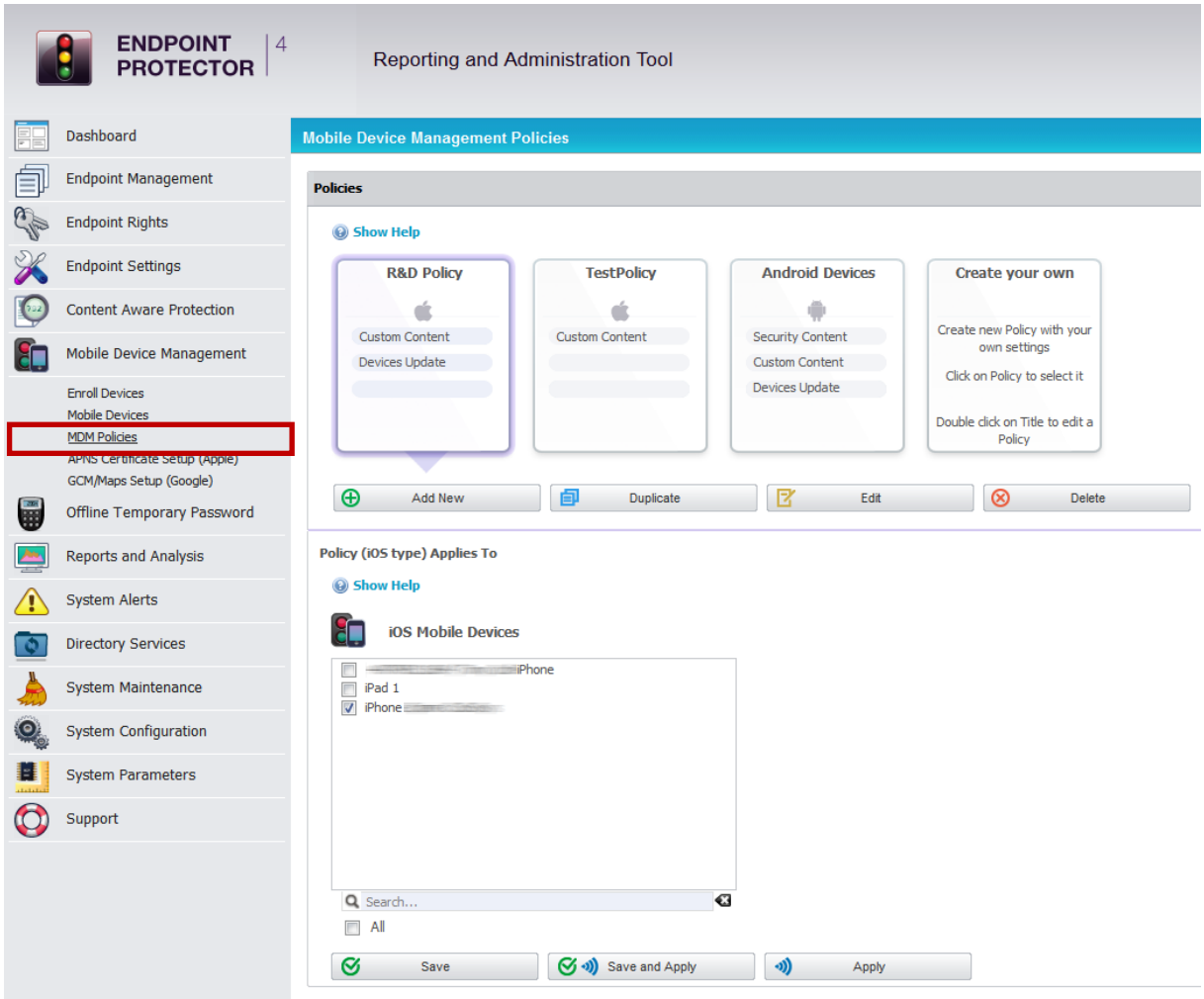
All installed Apps on an Android device are displayed in the "Installed Apps" tab.



To remove an app click the icon and the app will be deleted from the Android device. When a managed app is removed on the device the device user is not asked to confirm the removal of the app.

14. Policy Builder for iOS, OSX or Android Devices

The Policy Builder for iOS, OS X and Android devices is located under Mobile Device Management > MDM Policies.



The advantage of using an MDM Policy is that for a large number of devices the policy can be changed simultaneously.

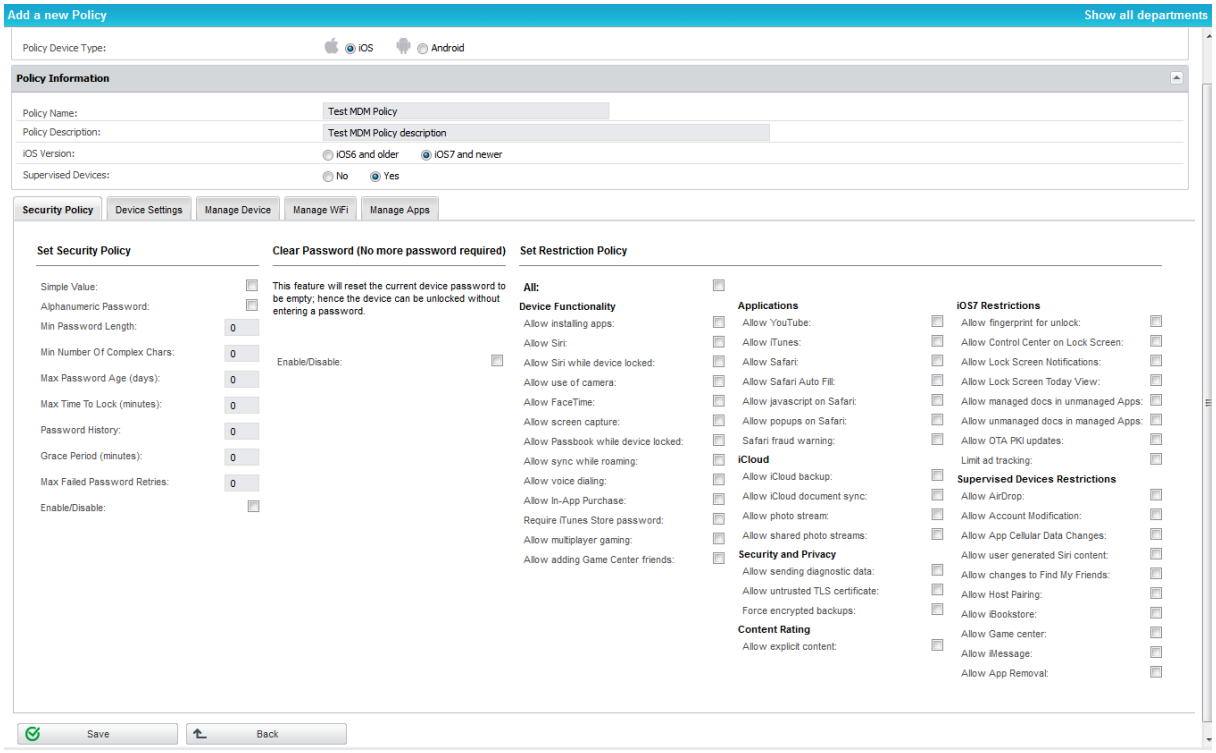
14.1. Create a Policy for iOS, OS X or Android Devices

To create a new MDM Policy click on "Add New" and then select for what operating System the Policy should apply. Choose between iOS, OS X and Android.

Give the policy a name and a description that will help you later manage your devices easier.

Policies are based on device operating system.

Make the settings for the policy you require. For each operating system different options are available to be set in the policy.



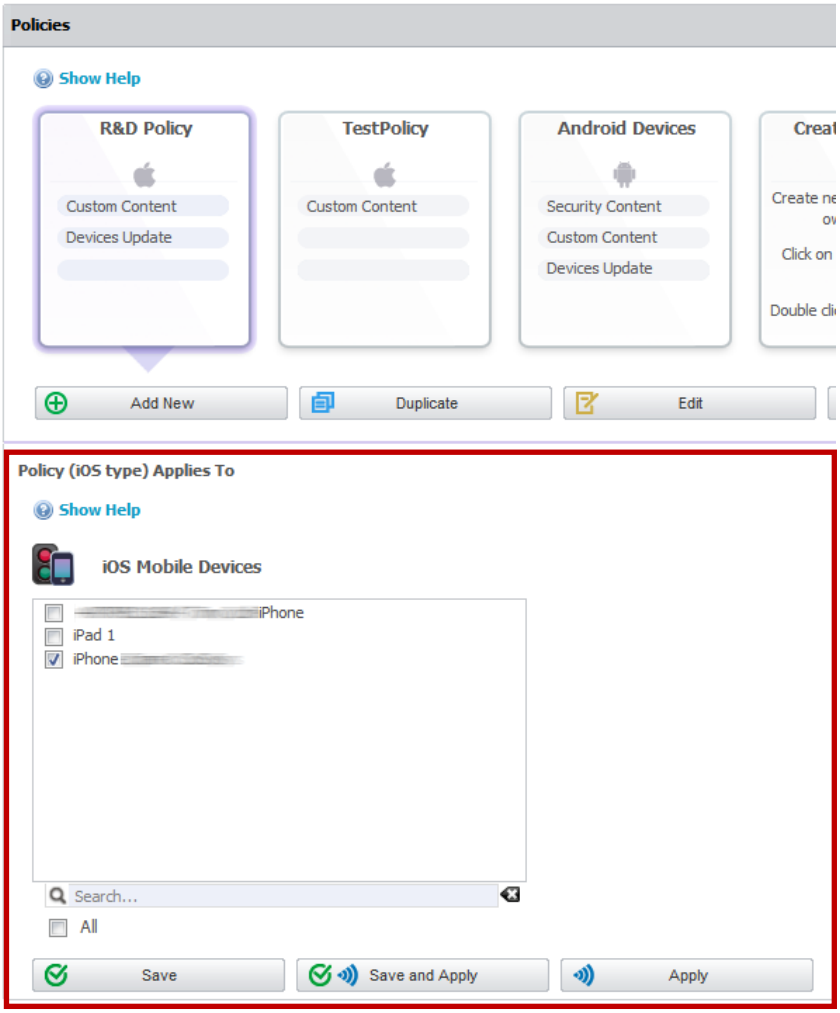
After you made the settings to the Policy click "Save".

Note!

If you select "iOS7 and newer" as your Operating System version but actually the devices Operating System is older than iOS6, the iOS7 Restrictions and Supervised Devices Restrictions won't be sent to the device.

14.2. Assigning Devices to Policy

After you created an MDM Policy you can assign devices to the policy by selecting them under "Policy (OS type) Applies To"



You can save your selection of devices by clicking "Save". The "Save" option is not yet applying the settings from the policy to a device. Only after you click "Apply" or "Save and Apply" the policy will be applied to the devices included in the policy.

15. Unmanage a Mobile Device / Uninstall App

In case that a mobile device must no longer be remotely managed/controlled, Endpoint Protector the user (depending on rights) and Endpoint Protector Administrator can uninstall / unmanage the mobile device. The uninstall/ unmanage process for Android and iOS/ OS X mobile devices is different.

15.1. iOS and OS X Device Unmanage by Administrator (over-the-air)

To unmanage an iOS or OS X device the Endpoint Protector Enrollment Profile on the iOS/ OS X device has to be removed. The Endpoint Protector Administrator can remove the profile by following the removal of profile information described in paragraph 9.14.1 (iOS)/10.11.1 (OS X). To unmanage a device it is important that the Endpoint Protector Enrollment Profile is removed. After removing of the Enrollment Profile the device status as described in chapter 8.1 Mobile Device Status will change to "MobileProfileRemoved".

15.1.1. iOS Uninstall / Unmanage by User (on Device)

To unmanage an iOS device, the Endpoint Protector Enrollment Profile on an iOS mobile device must be removed. Go to Device Settings -> General and select the Endpoint Protector Profile. The next displayed window will contain the option to "Remove" Endpoint Protector from the mobile device.

Attention!

Although the uninstallation can be performed by the user, the Administrator will also be notified about the removal of the Endpoint Protector Enrollment Profile.

15.1.2. OS X Uninstall / Unmanage by User (on Device)

To unmanage an OS X device, the Endpoint Protector Enrollment Profile on an OS X mobile device must be removed. Go to System Preferences ->Profiles and select the Endpoint Protector Profile and choose to remove it.

Attention!

Although the uninstallation can be performed by the user, the Administrator will also be notified about the removal of the Endpoint Protector Enrollment Profile.

15.2. Uninstall iOS EPP MDM app

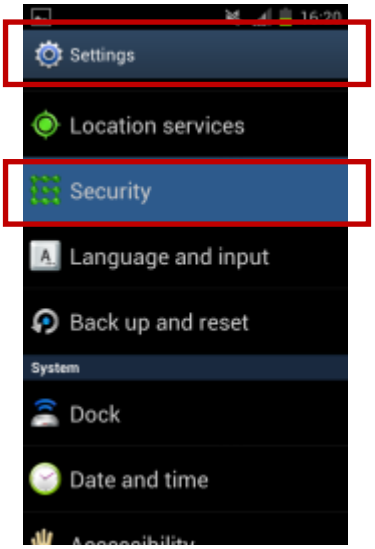
To uninstall the EPP MDM iOS app the user of the iOS device can uninstall it by pushing the EPP MDM app icon for two seconds and then deleting the app by clicking (x).

15.3. Android EPP Client App Uninstall / Unmanage Android Device

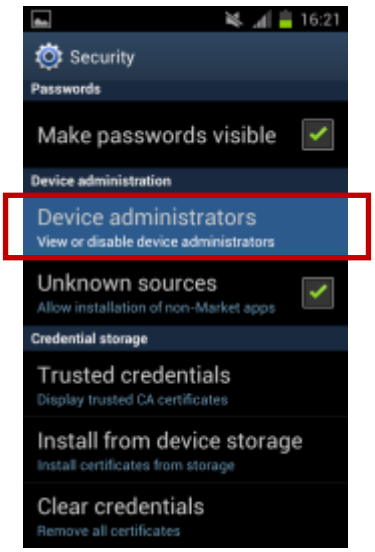
To uninstall EPP Client App on an Android Mobile Device, the user needs to disable the Device Administrator role from Device Settings.

To uninstall the EPP Client App follow these steps:

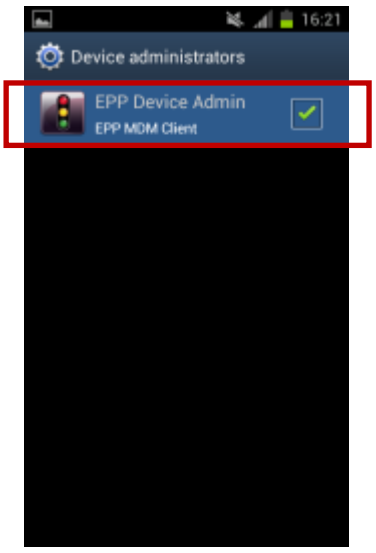
1. Go to “Settings” on your Android device and select “Security”.

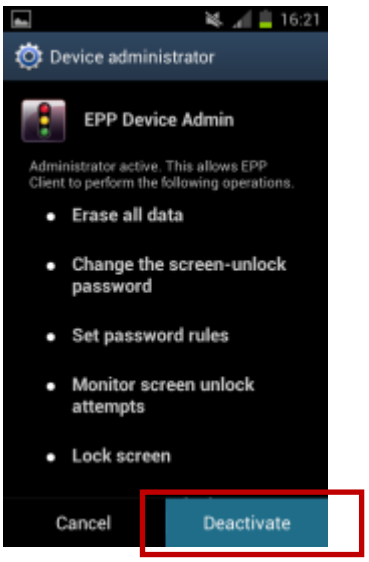


2. In "Security" select "Device administrators" and click on it.

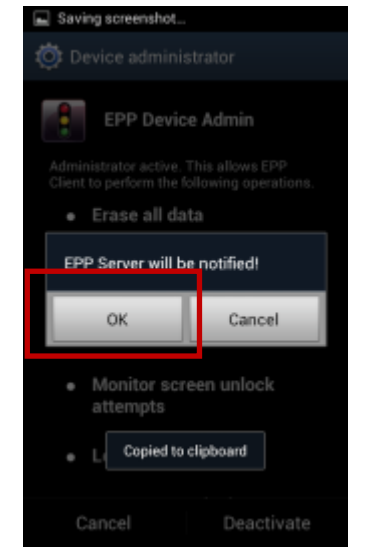


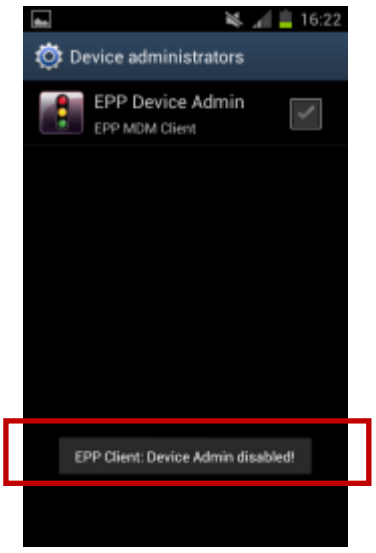
3. Select "EPP Device Admin" and click "Deactivate".



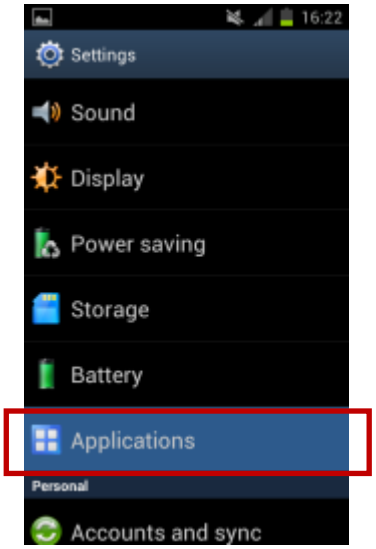


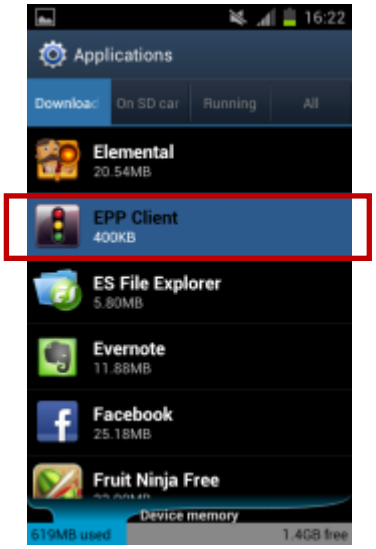
4. A pop-up will appear saying that the "EPP Server will be notified". To continue click "OK". A message saying "EPP Client Device Admin disabled" will appear.



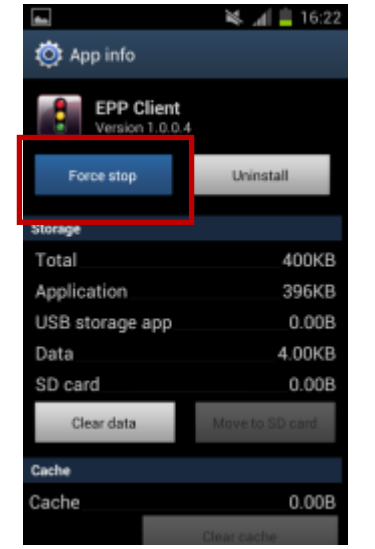


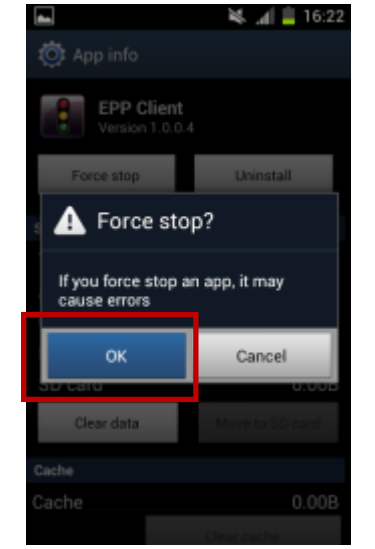
5. Now go to the "Application" menu on your Android device and locate "EPP Client" in the list of Applications. Click on "EPP Client".



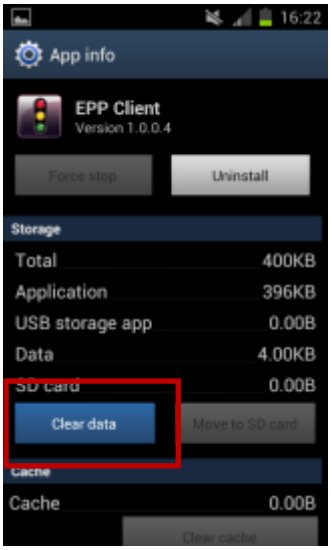


6. Click on "Force stop" and confirm the warning with "OK".

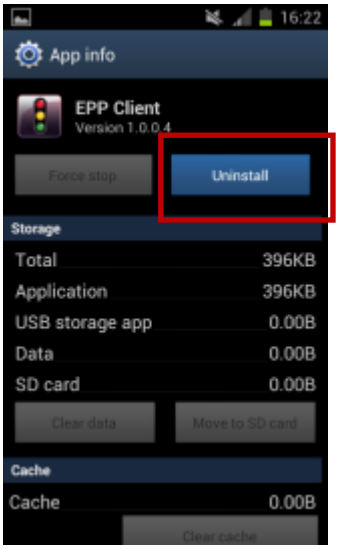


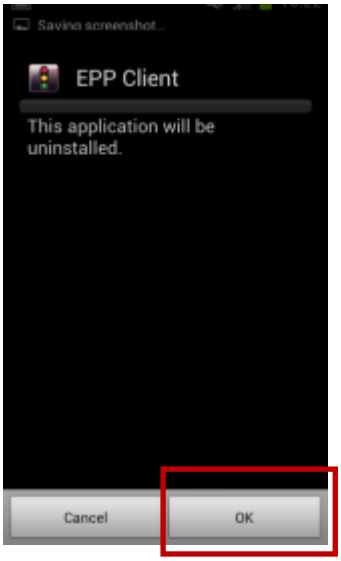


7. Now select "Clear data".

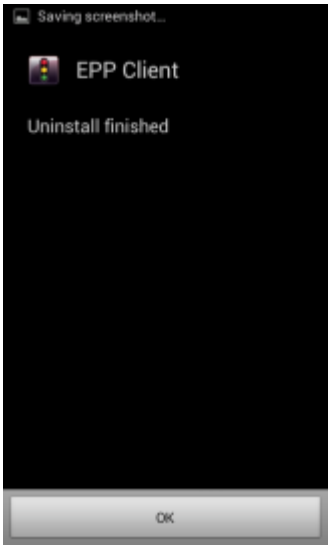


8. Now click "Uninstall" and confirm with "OK" the question if EPP Client should be uninstalled.





9. A message will indicate “Uninstall finished”, that the EPP Cient was now uninstalled from the Android device. Click “OK” and the process is finalized.

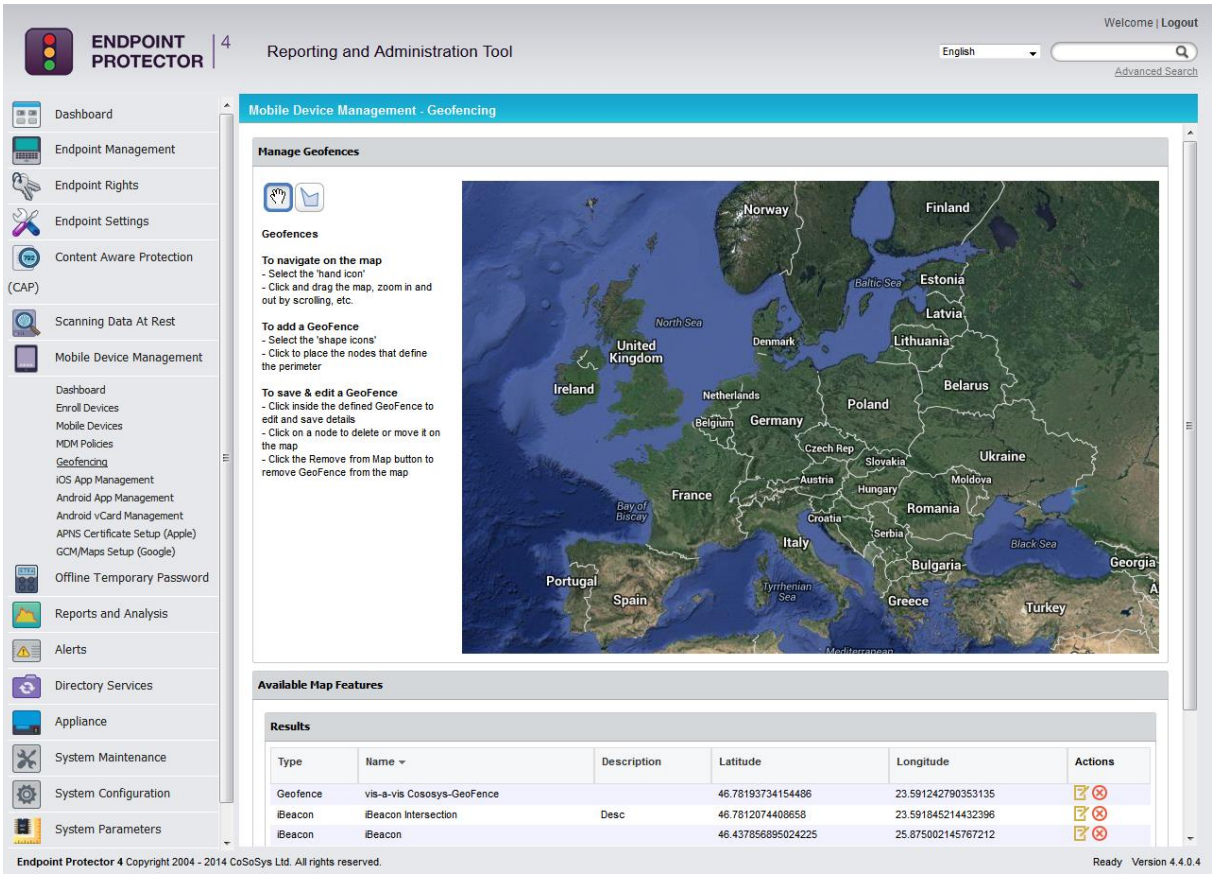


Attention!

Although the uninstallation can be performed by the user, the Endpoint Protector Appliance will also be notified about the removal of the Android EPP Client App.

16. GeoFencing

The Geofencing feature provides the option to define a virtual perimeter on a geographic area using a location-based service. This provides a better management of MDM Policies that apply only in a specific area.



16.1. How to setup a GeoFence

Setting up the virtual perimeter is simple and intuiteve.

To navigate on the map follow these steps:

1. Select the hand icon
2. Click and drag the map to the desired location
3. Zoom in and out using the mouse scroll

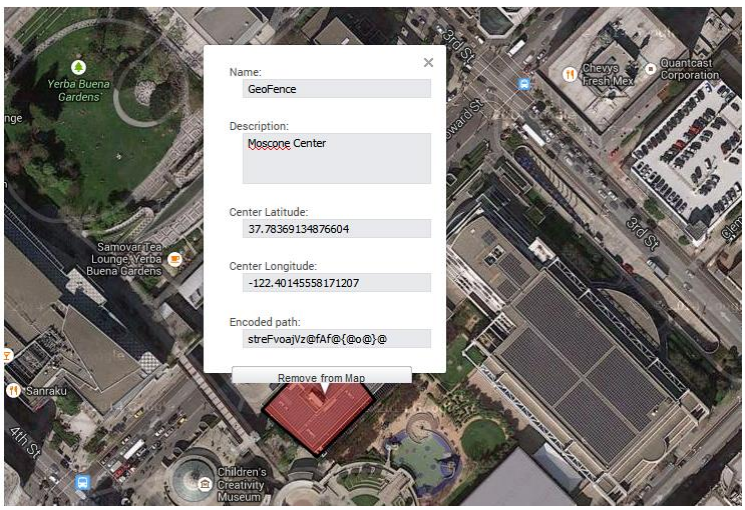
To add a GeoFence follow these steps:

1. Select the shape icon
2. Click to place the nodes that define the perimeter

To save and edit a GeoFence follow these steps:

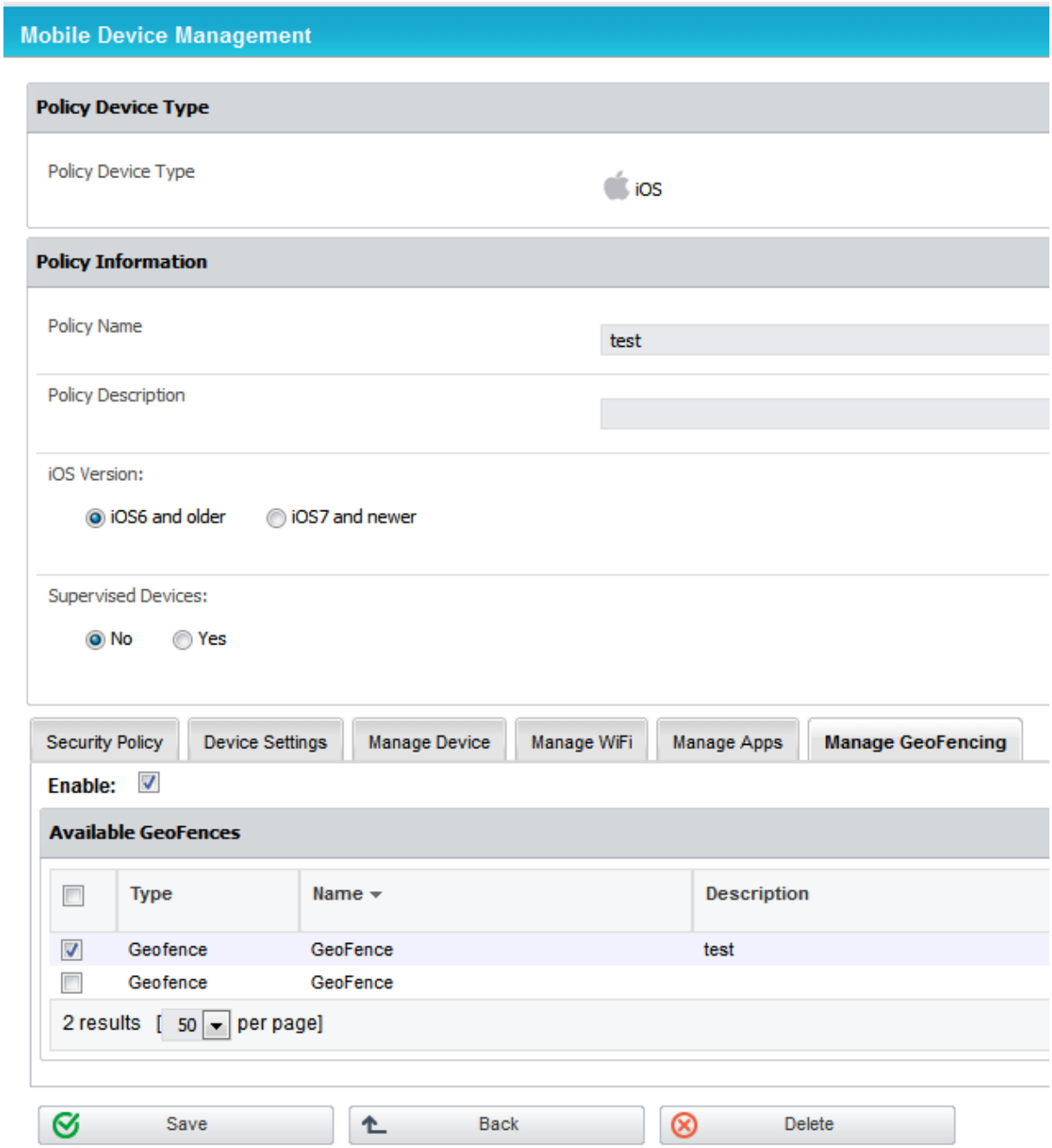
1. Click inside the above defined perimeter to edit and save details
2. Click on a node to delete or remove it from the map
3. Click on the Remove from Map button to remove GeoFence from the map
4. Click the Save Geofence Data to save the virtual perimeter

When a Geofence has been created, there are several details that are displayed to provide a better insight like Latitude and Longitude. There is also an optional Description field, recommended for a better management of the area and setting that apply to it.



16.2. How to deploy MDM Policies using Geofences

Once the virtual perimeter has been defined, pushing specific settings through Geofencies can be done from the MDM Policies.



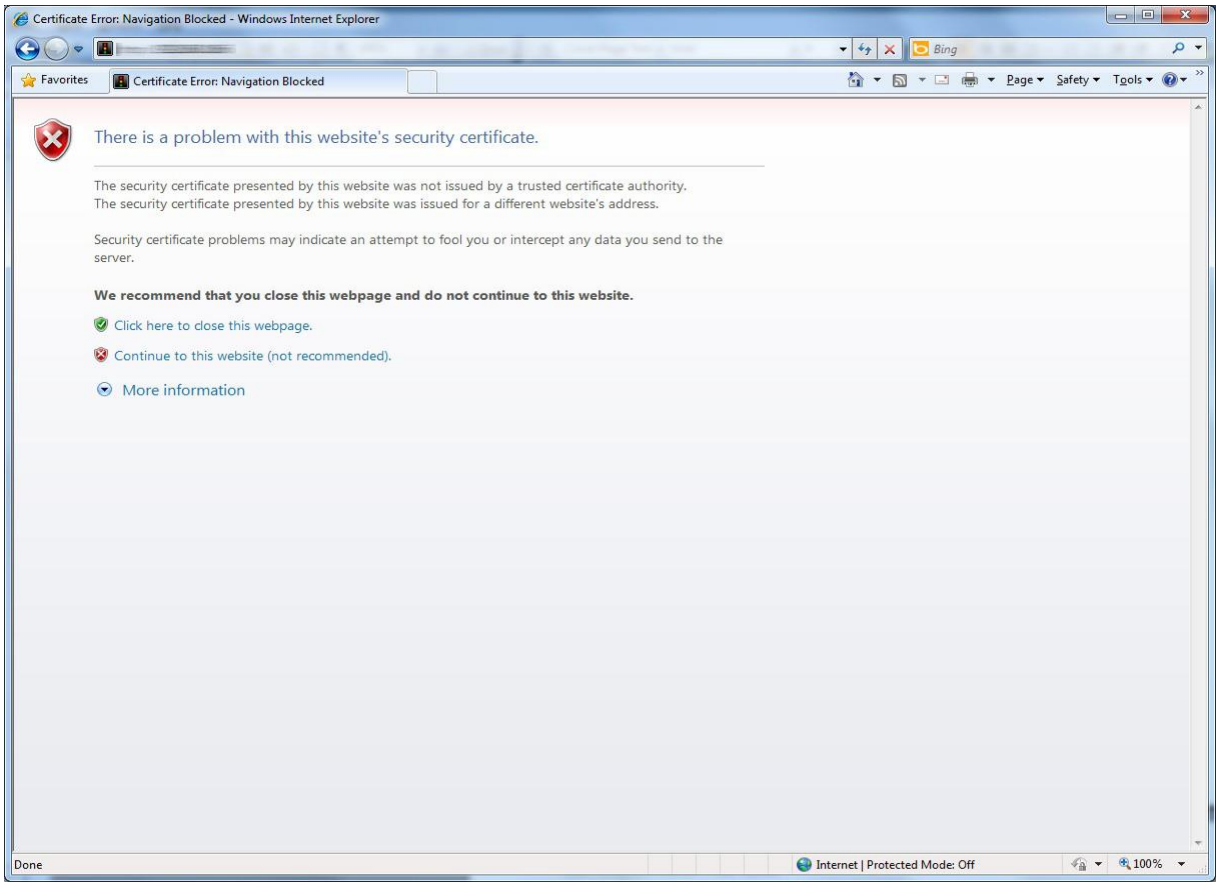
All off the settings previously defined in the Security Policy, Device Settings, Manage Device, Manage WiFi and Manage Apps tabs will apply to that specific Geofence.

17. Installing Root Certificate to your Internet Browser

17.1. For Microsoft Internet Explorer

Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example https://192.168.0.201).

If there is no certificate in your browser, you will be prompted with Certificate Error page like the screenshot below.


Certificate Error: Navigation Blocked - Windows Internet Explorer
Favorites
Certificate Error: Navigation Blocked
Page
Safety
Tools
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information
Done
Internet | Protected Mode: Off
100%

Continue your navigation by clicking "Continue to this website (not recommended)".

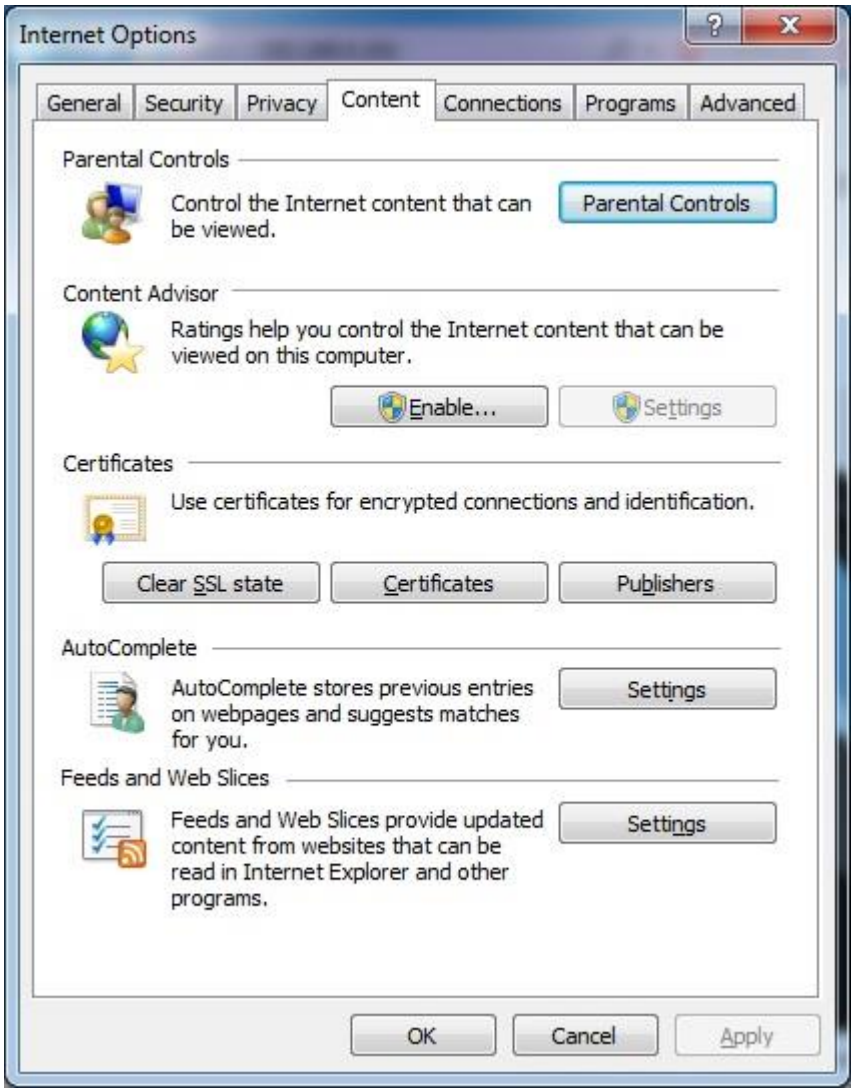
Now, go to the Certificate file you downloaded from the Appliance Setup Wizard->Appliance Server Certificate-> and install the Certificate.

Click the Certificate Error button just next to the IE address bar as shown.

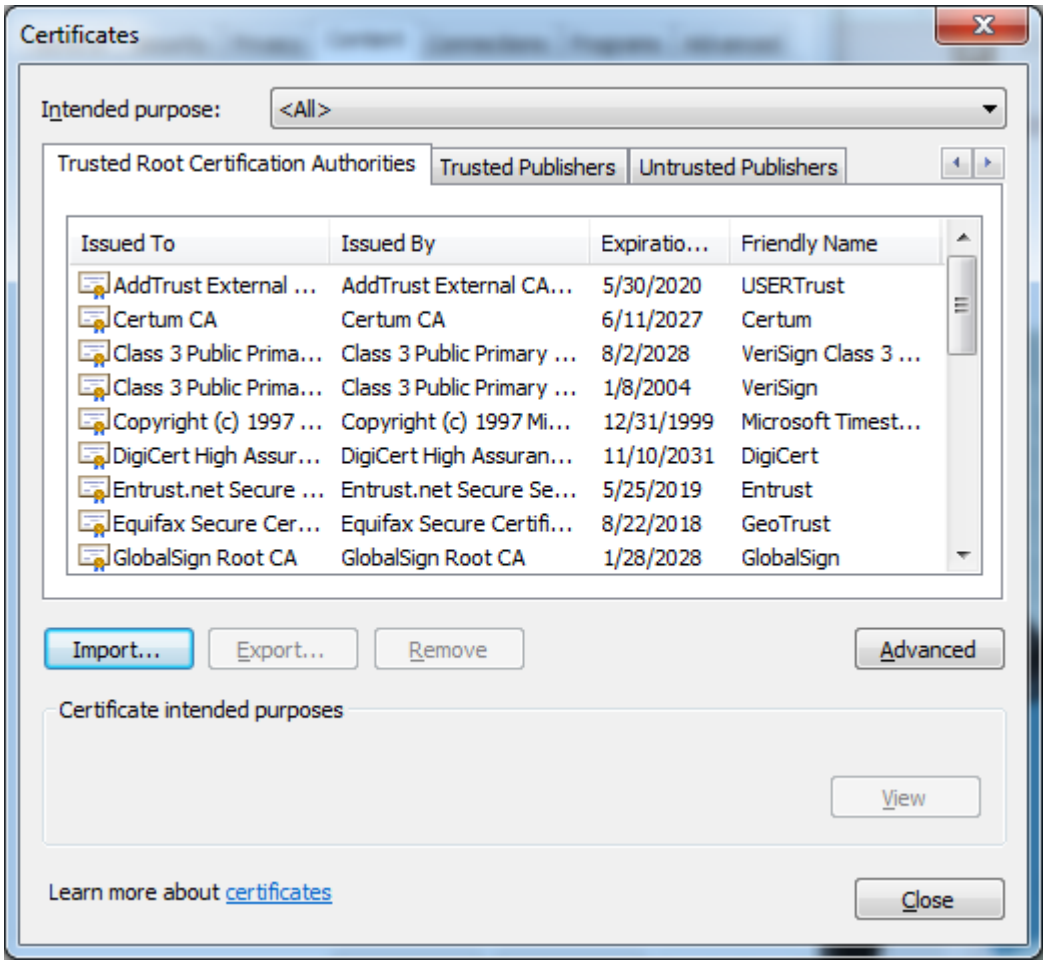
By clicking the "Certificate Error" button, a pop-up window appears. Just click the "View certificates" in that pop-up window.

Another pop-up Certificate window will appear with three tabs namely "General", "Details" and "Certification Path".

Select the "General" tab and then click "Install Certificate..." button or go to Tools->Internet Options-> Content->Certificates.



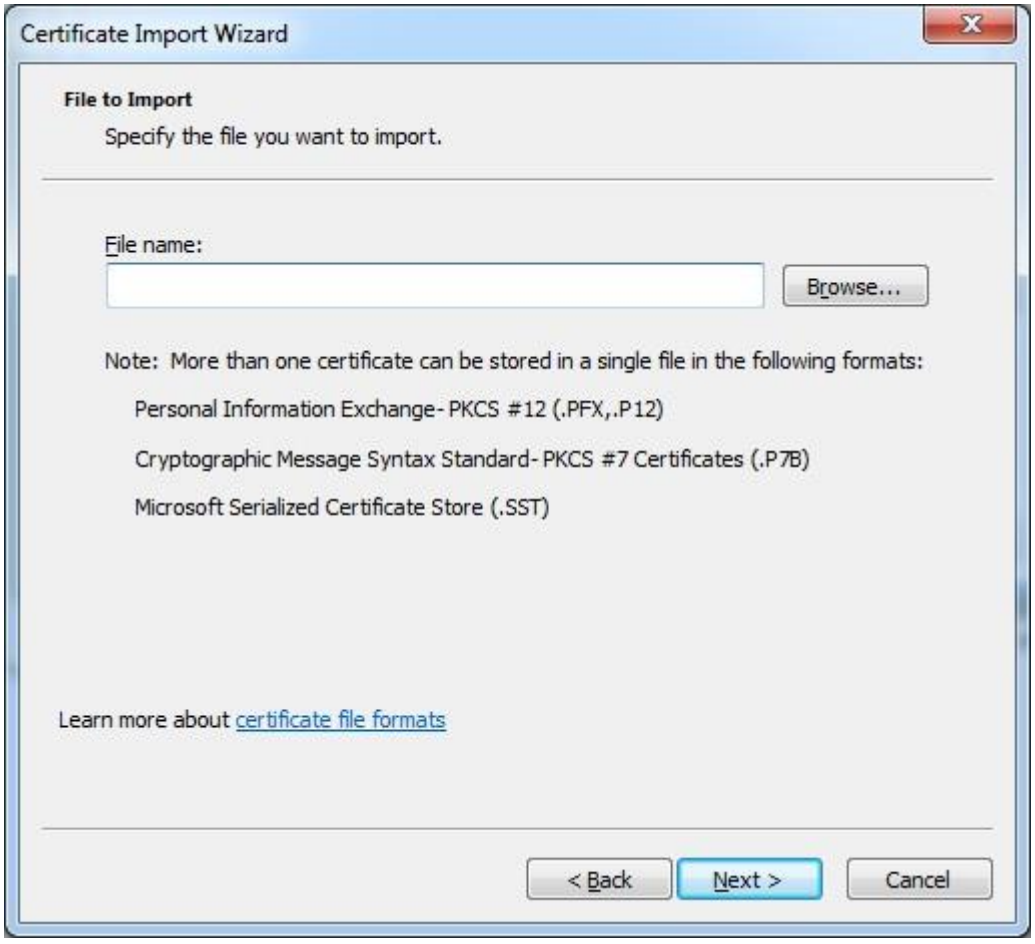
From the Certificates list, select "Trusted Root Certification Authorities" and click on the "Import" button.



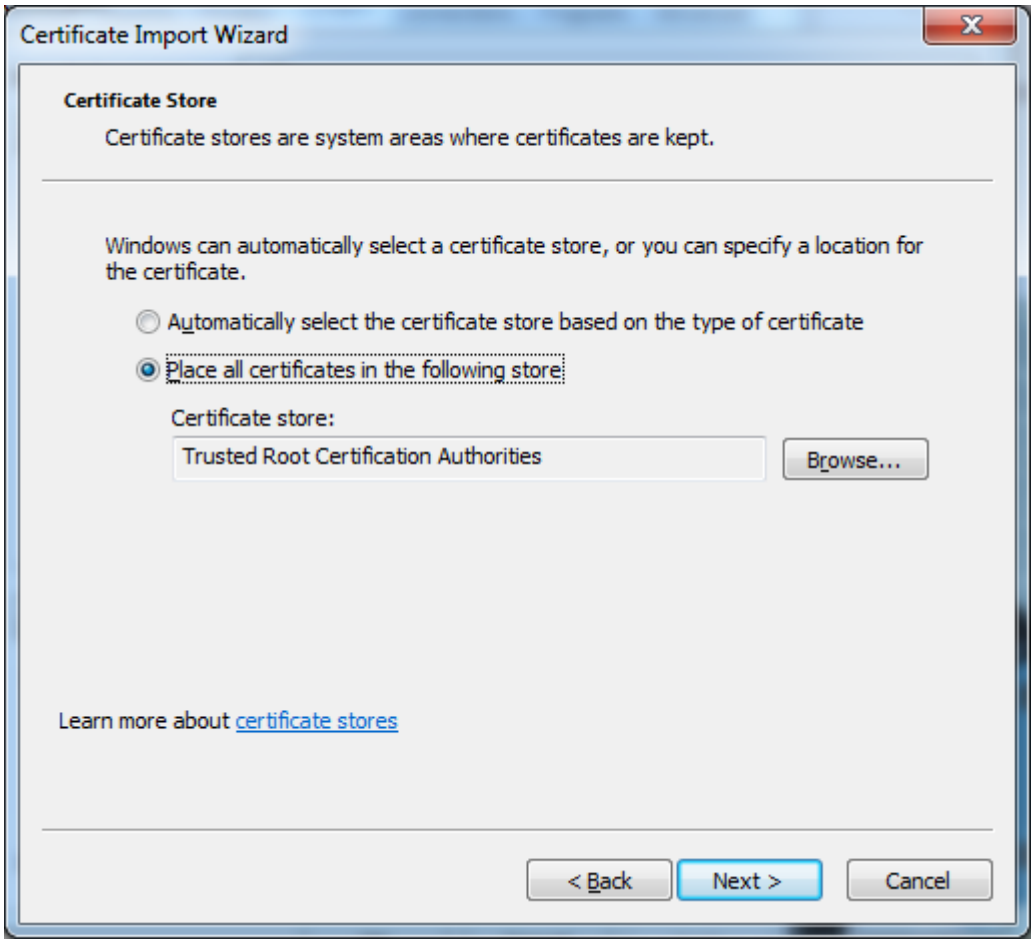
A Welcome to the Certificate Import Wizard pops up. Just click the Next button.

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

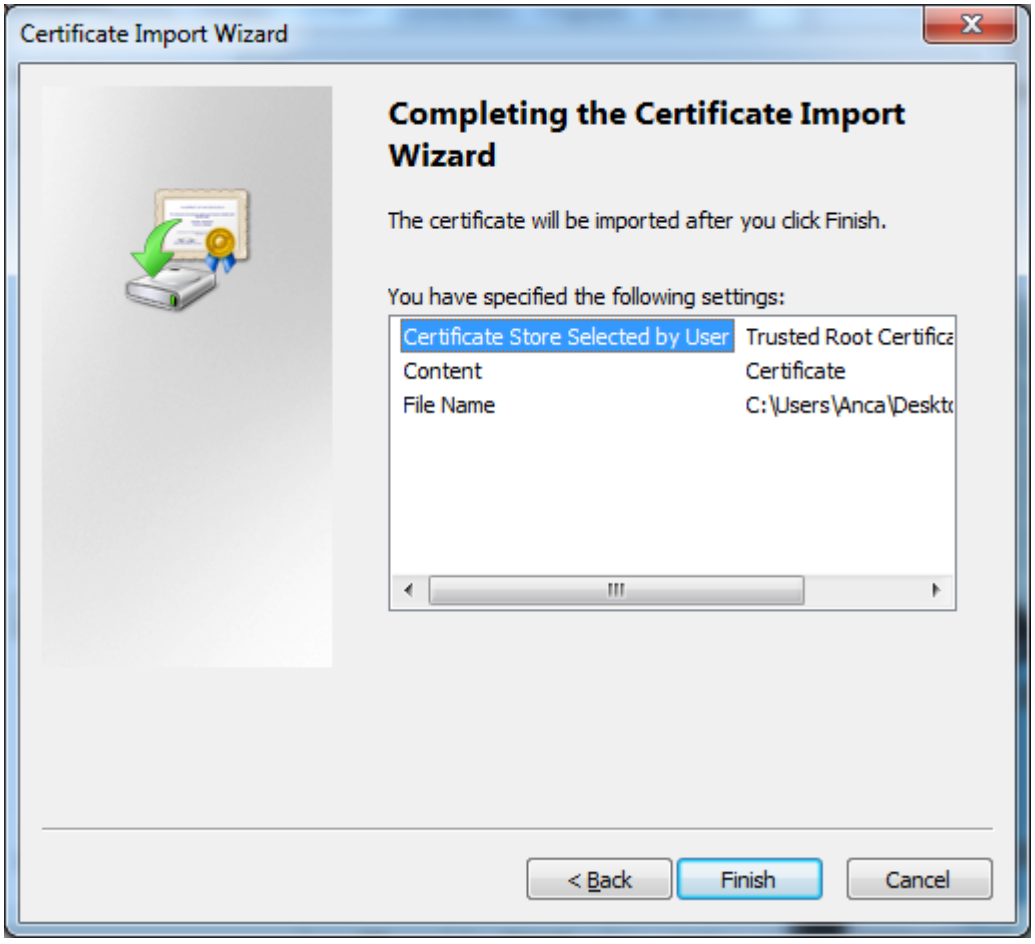
Browse for the Certificate file you downloaded from the Appliance Setup Wizard ->Appliance Server Certificate.


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Learn more about certificate file formats
< Back
Next >
Cancel

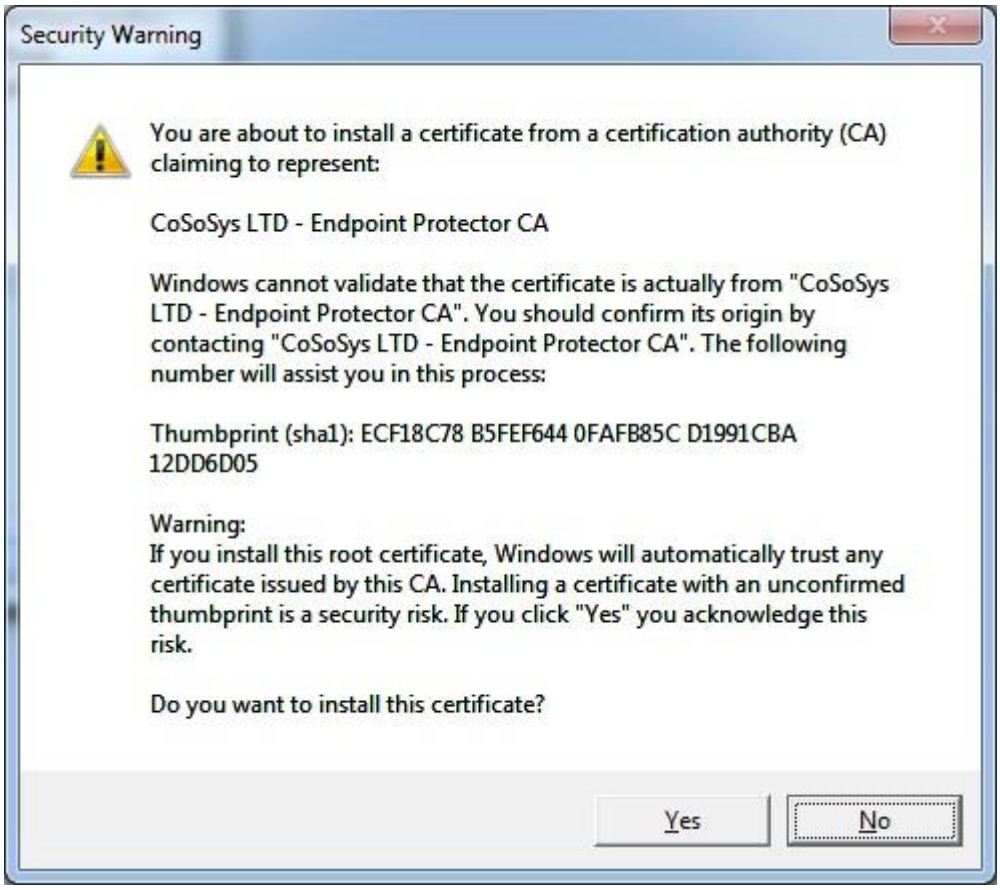
In the Certificate Store window, select “Place all certificates in the following store” radio button.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

Another "Completing the Certificate Import Wizard" pops up. Just click the "Finish" button.

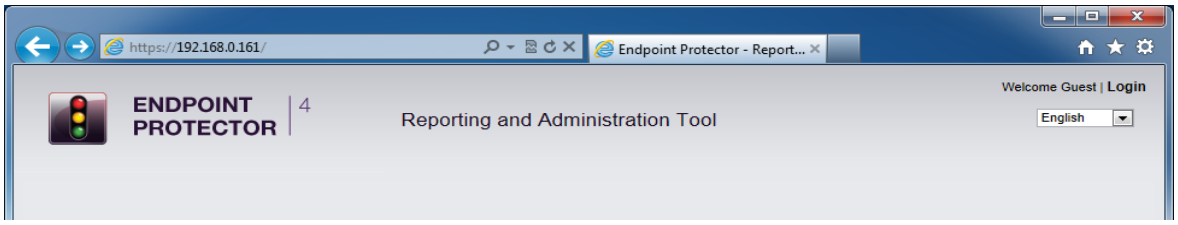


A Security Warning window pops up. Just click "Yes".


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
CoSoSys LTD - Endpoint Protector CA
Windows cannot validate that the certificate is actually from "CoSoSys LTD - Endpoint Protector CA". You should confirm its origin by contacting "CoSoSys LTD - Endpoint Protector CA". The following number will assist you in this process:
Thumbprint (sha1): ECF18C78 B5FEF644 0FAFB85C D1991CBA 12DD6D05
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

You have now successfully installed the Certificate.

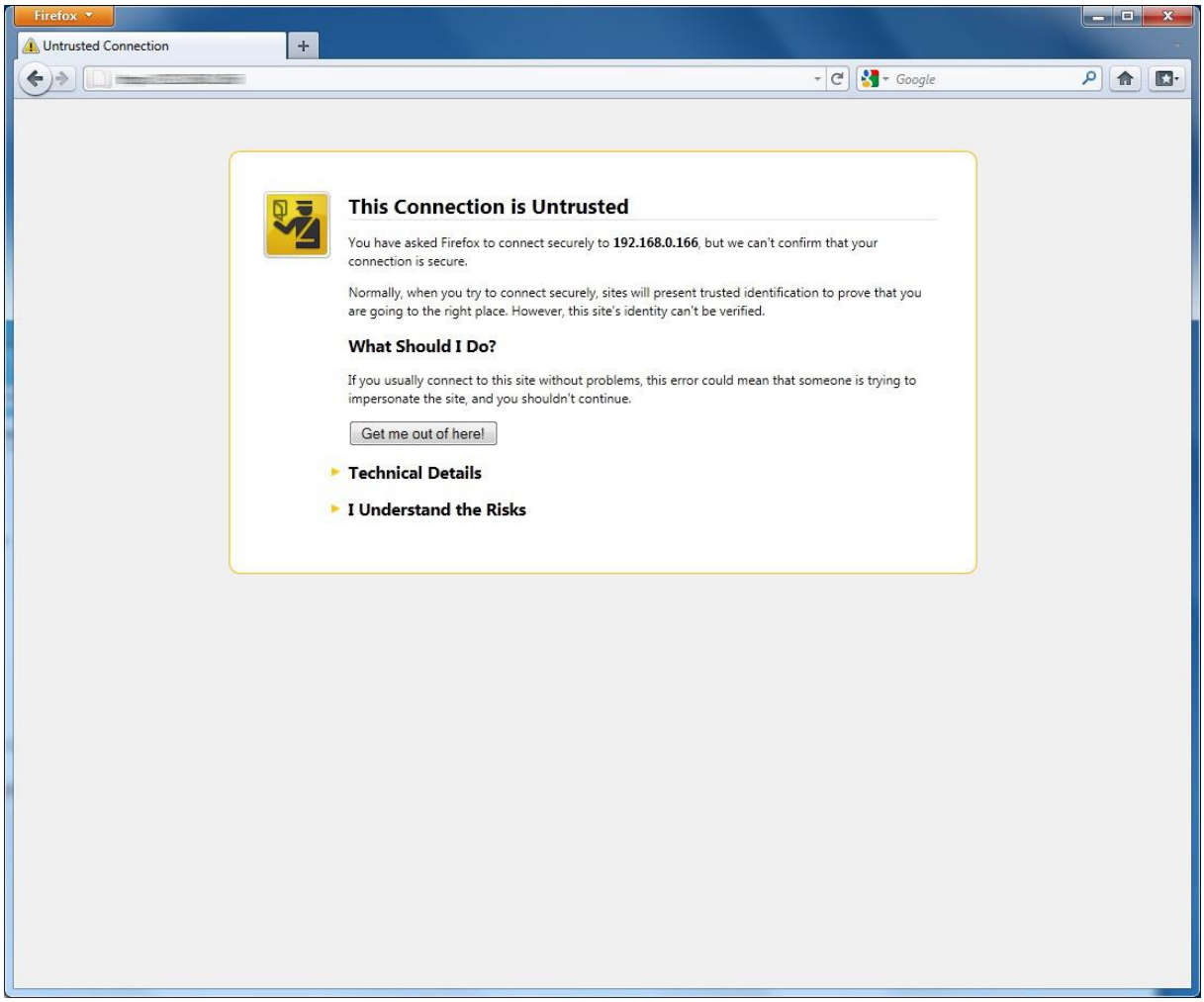
Close the Internet Explorer browser and try accessing the Endpoint Protector Administration and Reporting Tool IP address again.



17.2. For Mozilla Firefox

Open the Browser.

Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example https://192.168.0.201).


Firefox
Untrusted Connection
Google
This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.0.166, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

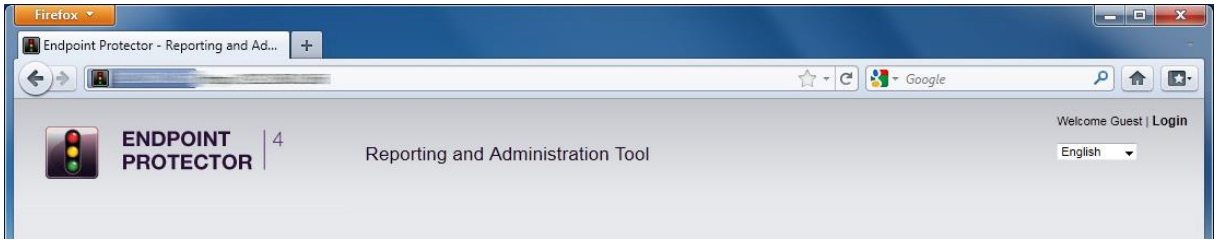
From the above screenshot This Connection is Untrusted, choose I Understand the Risks. Click Add Exception.

Security Warning window pops up.

Just click Get Certificate button and then the Confirm Security Exception button.

Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location:
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

Close the browser and start it again.



18. Terms and Definitions

Here you can find a list of terms and definitions that are encountered throughout the user manual.

18.1. Server Related

Appliance – Appliance refers to the Endpoint Protector Appliance which is running the Endpoint Protector Server, Operating System, Databases, etc.

Computers – refers to PC's, workstations, thin clients, notebooks which have Endpoint Protector Client installed.

Devices – refers to a list of known mobile devices, ranging from iPhones, iPads and MacBooks to Android Smartphones and tablets.

Groups – can be groups of devices, users or computers. Grouping any of these items will significantly help the server administrators to easily manage rights and settings for them.

Departments – an alternative way to Groups to organize main entities (devices, users or computers), which involves also the administrators of Endpoint Protector.

Mobile Device Management (MDM) – a set of software and services that allow organizations to closely monitor, manage and secure employees' mobile devices regardless of the different mobile service providers and mobile operating systems being used.

BYOD – acronym that stands for "Bring Your Own Device", which refers to the new trend adopted by employees to take their own personal devices to work and directly interface to the corporate network.

Apple APNs Certificate – stands for Apple Push Notification Service and it is a certificate signed by Apple that enables the management of iOS and OS X devices by IT Administrators using available MDM software

Provisioning – refers to the process of providing mobile device users with appropriate access to all necessary enterprise resources and enforcement of company policies.

Enrollment – for mobile devices, it refers to the setup process for enabling Mobile Device Management for a specific mobile phone or tablet.

18.2. Client Related

Endpoint – can be a Personal Computer, a Workstation you use at the office or a Notebook. An endpoint can call and be called. It generates and terminates the information stream.

Client - refers to the client user who is logged in on a computer and who facilitates the transaction of data.

Rights – applies to computers, devices, groups, users and global rights; it stands for privileges that any of these items may or may not possess.

Online computers – refers to PC's, Workstations and/or Notebooks which have Endpoint Protector Client installed and are currently running and are connected to the Endpoint Protector server.

Connected devices – are devices which are connected to online computers.

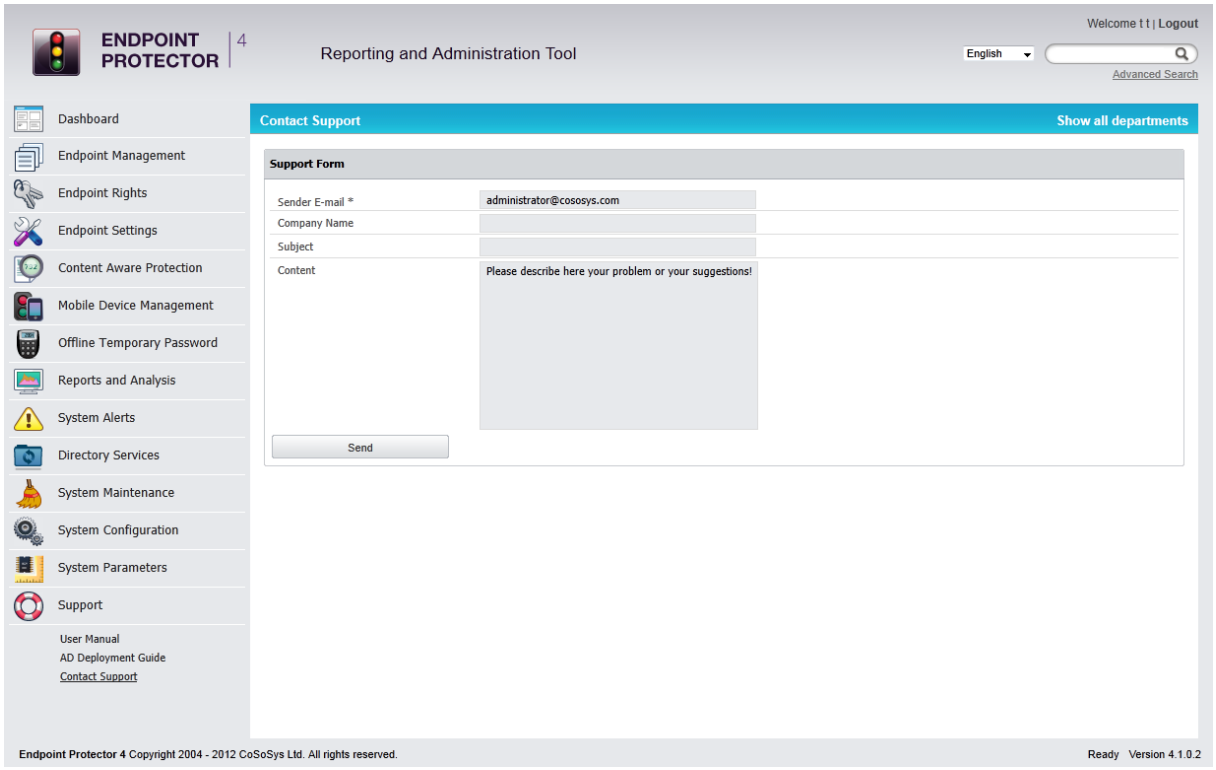
Events – are a list of actions that hold major significance in Endpoint Protector. There are currently 17 events that are monitored by Endpoint Protector:

- Connected – the action of connecting a device to a computer running Endpoint Protector Client.
- Disconnected – the action of (safely) removing a device from a computer running Endpoint Protector Client.
- Enabled – refers to devices; the action of allowing a device access on the specified computer(s), group(s) or under the specified user(s).
- Disabled – refers to devices; the action of removing all rights from the device, making it inaccessible and therefore unusable.
- File delete – a file located on a portable device has been deleted.

19. Support

In case additional help, such as the FAQs or e-mail support is required, please visit our support website directly at http://www.endpointprotector.com/support/.

You can also write an e-mail to our Support Department under the Contact Us tab from the Support module.



One of our team members will contact you in the shortest time possible.

Even if you do not have a problem but miss some feature or just want to leave us general comment we would love to hear from you. Your input is much appreciated and we welcome any input to make computing with portable devices safe and convenient.

20. Important Notice / Disclaimer

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2014 CoSoSys Ltd.; Endpoint Protector, My Endpoint Protector are trademarks of CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. Android is registered trademark of Google Inc. Macintosh, Mac OS X, iOS, MacBook, are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.